



# **BiPAC 8200N**

## **802.11n VDSL2 Firewall Router**

### **User Manual**

# Table of Contents

<b>Chapter 1: Product .....</b>	<b>1</b>
Introduction to your Router.....	1
Features .....	4
Hardware Specifications .....	5
<b>Chapter 2: Product Overview.....</b>	<b>6</b>
Package Contents.....	6
Important note for using this router .....	6
Device Description .....	7
The Front LEDs.....	7
The Rear Ports .....	8
Cabling.....	10
<b>Chapter 3: Basic Installation .....</b>	<b>11</b>
Applications of the device .....	12
Network Configuration.....	13
Configuring PC in Windows 7 .....	13
Configuring PC in Windows Vista.....	15
Configuring PC in Windows XP.....	17
Configuring PC in Windows 2000 .....	18
Configuring PC in Windows 95/98/Me.....	19
Configuring PC in Windows NT4.0.....	20
Factory Default Settings.....	21
Information from your ISP .....	22
<b>Chapter 4: Configuration .....</b>	<b>23</b>
Easy Sign-On (EZSO).....	23
Configuration via Web Interface.....	26
Quick Start .....	27
Basic Configuration Mode.....	34
Status.....	34
WAN – Main Port: VDSL .....	35

Obtain IP Address Automatically (VDSL) .....	35
Fixed IP Address (VDSL) .....	36
PPPoE Connection (VDSL) .....	37
Pure Bridge (VDSL) .....	38
WAN – Main Port: EWAN .....	39
Obtain IP Address Automatically (EWAN) .....	39
Fixed IP Address (EWAN) .....	40
PPPoE Connection (EWAN) .....	41
WLAN .....	42
<b>Advanced Configuration Mode .....</b>	<b>44</b>
Status .....	44
VDSL Status .....	46
ARP Table .....	47
DHCP Table .....	48
System Log .....	49
Firewall Log .....	50
UPnP Portmap .....	51
Configuration .....	52
LAN - Local Area Network .....	53
WAN - Wide Area Network .....	73
System .....	82
Firewall .....	89
QoS - Quality of Service .....	99
Virtual Server .....	104
Time Schedule .....	110
Advanced .....	111
Save Configuration to Flash .....	126
Restart .....	127
Logout .....	128
<b>Chapter 5: Troubleshooting .....</b>	<b>129</b>
<b>Appendix: Product Support &amp; Contact .....</b>	<b>130</b>

# Chapter 1: Product

## Introduction to your Router

Thank you for purchasing BiPAC 8200N Router. Your new router is an all-in-one unit that combines a VDSL modem, VDSL2 router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over a VDSL broadband connection.

The BiPAC 8200N is an all-in-one VDSL2 Router with the latest 802.11n technology. It is designed for home and SOHO users who seek extreme mobility, high-speed wireless connection and better wireless coverage while maintaining high-speed broadband access with VDSL2.

The BiPAC 8200N is capable of offering optimal speeds and coverage over the integrated wireless 802.11n access point. The device supports the highest rate of up to 100Mbps/100Mbps in VDSL2 Profile (30a). Since VDSL2 has the characteristic of faster rates over shorter distances, the ideal architecture for Telcoms is to use fiber optic lines as the backbone and a VDSL2 line as the last mile into the home or office. VDSL2 operates over copper wires so that telecom operators can provide bundled services to end-users similar to those that cable operators offer.

With outstanding throughput, the BiPAC 8200N can complement a fiber network to offer the best solution for delivering IPTV or home entertainment services. The SOHO Firewall is integrated to provide protection against hacker attacks while the Quality of Service prioritizes queues and traffic for applications such as music downloads, online gaming, video streaming and file sharing.

### **Express Internet Access – VDSL2 capable**

The router complies with VDSL worldwide standards. Supporting downstream rates of 100Mbps with VDSL and upstream rates of 100 Mbps. Users enjoy not only high-speed VDSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio which are easier and faster than ever. The router is compliant with ITU-T VDSL2 Standard G.993.2, G.994.1 and G.997.1. Support VDSL2 Profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a.

### **802.11n Wireless AP with WPA Support**

With an integrated 802.11n Wireless Access Point in the router, the device delivers up to 6 times faster speeds and 3 times farther range than an 802.11b/g wireless network. It supports a fast data transfer rate up to 300Mbps and is fully compatible with 802.11b/11g equipments. The supported features of Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) enhance the security level of data protection and access control via Wireless LAN. The router also supports Wi-Fi Protected Setup (WPS) that features the establishment of a secured wireless network. The built-in Wireless Distribution System (WDS) also facilitates the flexibility for wireless network expansion without the need for any external wires or cables.

### **Fast Ethernet Switch**

A 4-port 10/100Mbps fast Ethernet switch is built-in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports, with auto detection allowing you to use either straight or cross-over Ethernet cables.

## **EWAN**

Besides using VDSL to get connected to the Internet, this router offers its Ethernet port 4 as a WAN port to be used to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online.

### **Multi-Protocol to Establish a Connection**

The router supports PPP over Ethernet, DHCP Client and Fixed IP address to establish a connection with an ISP.

### **Universal Plug and Play (UPnP) and UPnP NAT Traversal**

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, you can seamlessly connect to Net Meeting or MSN Messenger.

### **Network Address Translation (NAT)**

It allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

### **Firewall**

NAT technology supports simple firewalls and provides options for blocking access from the Internet, like Telnet, FTP, TFTP, WEB, SNMP and IGMP.

### **Domain Name System (DNS) Relay**

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

### **Dynamic Domain Name System (DDNS)**

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like <http://www.dyndns.org/>. More than 5 DDNS servers are supported.

### **PPP over Ethernet (PPPoE)**

This device provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

## **Quality of Service (QoS)**

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by Internal IP address, External IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

## **Virtual Server**

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

## **Dynamic Host Configuration Protocol (DHCP) Client and Server**

In a WAN site, the DHCP client obtains an IP address from the Internet Service Provider (ISP) automatically. In a LAN site, the DHCP server allocates a range of client IP addresses, including subnet masks and DNS IP addresses and distributes them to local computers. This provides an easy way to manage the local IP network.

## **Rich Packet Filtering**

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.

## **Web-based GUI**

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

## **Firmware Upgradeable**

Device can be upgraded to the latest firmware through the WEB based GUI.

# Features

- Compliant with ITU-T G.993.2 , G.994.1 and G.997.1 VDSL2 Standard
- VDSL2 Profiles: 8a/b/c/d, 12a/b, 17a, 30a
- Band Plan 997 and 998 supported
- Annex A, Annex B, Annex C supported
- US0 Supported
- OLR Supported
- Compliant with VDSL2 MIB
- Integrated 4-port Ethernet Switch
- Ideal for LRE applications
- SOHO Firewall Security with DoS Prevention and Packet Filtering
- Universal Plug and Play (UPnP) Compliant
- Easy Sign-On (EZSO) and Web-based Configuration
- Quality of Service Control
- Easy Network Management
- High-speed wireless connection up to a 300Mbps data rate
- Expanded wireless coverage of up to 3 times the range of 802.11g products
- 802.11n Wireless AP with Wi-Fi Protected Setup (WPS), WPA-PSK/ WPA2-PSK support
- Multiple SSIDs
- Supports TR-069

# Hardware Specifications

## Physical Interface

- WLAN: 2 x antennae
- DSL: VDSL port
- Ethernet: 4-port 10/100Mbps auto-crossover (MDI / MDI-X) Switch
- Reset button
- WPS push button
- Power jack
- Power switch



# Chapter 2: Product Overview

## Package Contents

- 8200N 802.11n VDSL2 Firewall Router
- Antenna x 2
- CD containing the on-line manual
- RJ-11 xDSL / telephone cable
- Ethernet (RJ-45) cable
- Power adapter
- Quick Start Guide
- Splitter / Micro-filter (Optional)

## Important note for using this router



### Warning

- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this product and all accessories outdoors.

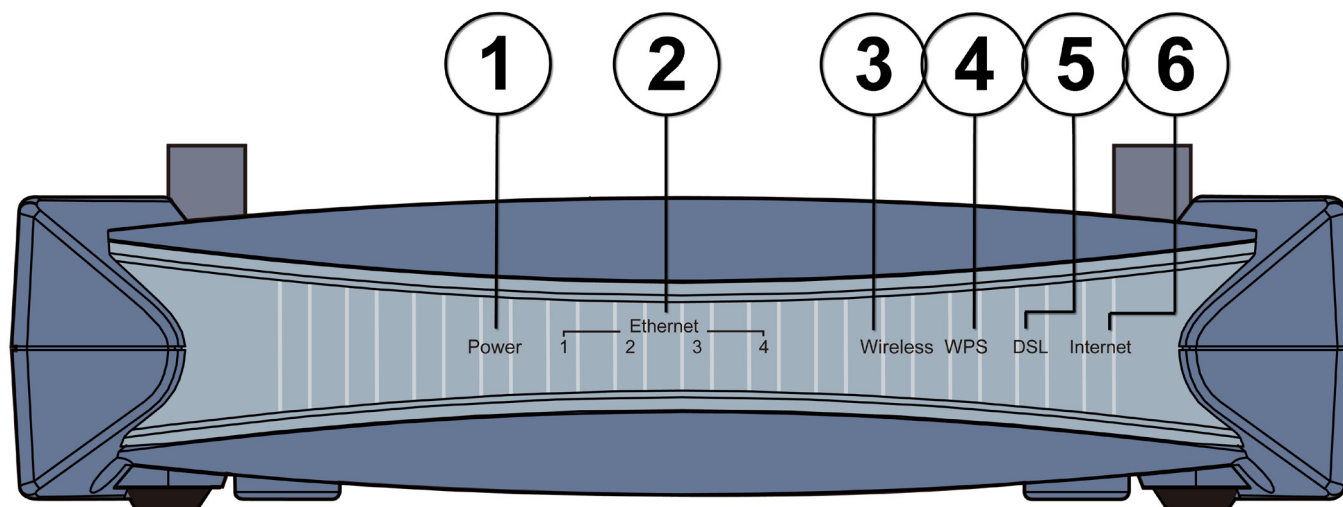


### Attention

- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

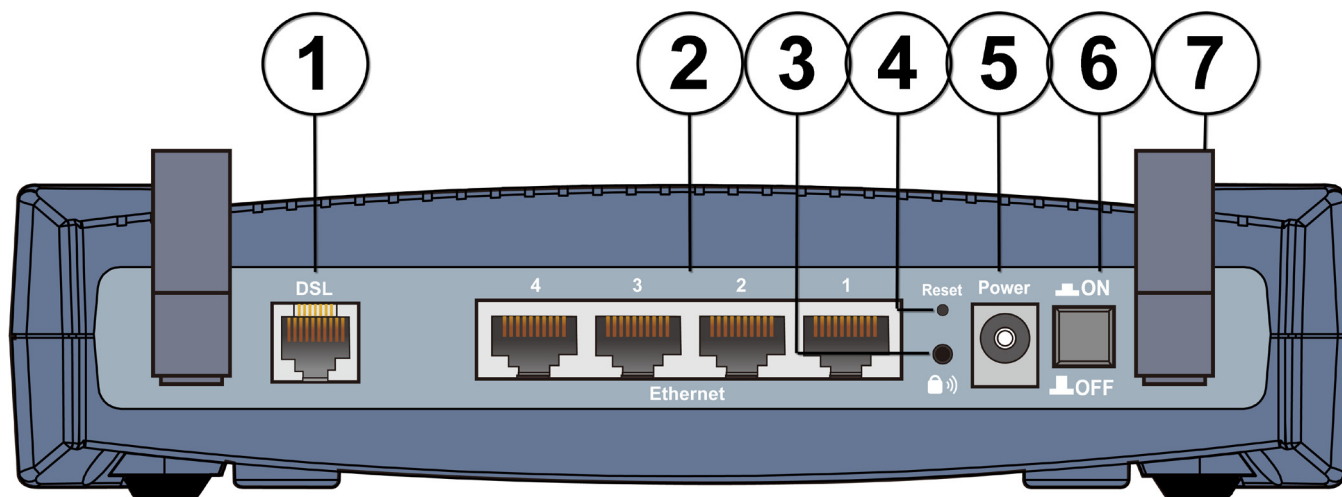
# Device Description

## The Front LEDs



LED		Meaning
1	Power	Lit red when the device is booting. Lit green when the system is ready. Flashes when the system is rebooting or firmware upgrading.
2	Ethernet port 1X — 4X (RJ-45 connector)	Lit when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission hits 100Mbps; Lit orange when the speed of transmission hits 10Mbps. Blinking when data is transmitted/received.
3	Wireless	Lit green when a wireless connection is established. Blinking when data is transmitted/received.
4	WPS	Lit green when a wireless connection is established. Blinking when WPS configuration is in progress.
5	DSL	Lit green when the device is successfully connected to an VDSL DSLAM. ("line sync")
6	Internet	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when the device is in bridge mode or when WAN connection absent.

## The Rear Ports



Port		Meaning
1	DSL	Connect this port to the VDSL/telephone network with the RJ-11 cable (telephone) provided.
2	Ethernet	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps. <b>Note: Only Ethernet port 4 can be used for EWAN.</b>
3	WPS	Push this button to trigger Wi-Fi Protected Setup function.
4	Reset	Press this button for more than 1 second to restore the device to its default mode.
5	Power	Connect it with the supplied power adapter.
6	Power Switch	Power ON/OFF switch.
7	Antenna	Connect the detachable antenna to this port.

## Recovery Operation

### 1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):

The system will check the firmware of this device automatically while turning on the modem. Once the firmware is not integrated, the system enters the recovery state. The modem emergency-reflash web interface will then be accessible via <http://192.168.1.254> where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

### 2. Recovery procedures for a lost web interface password:

After turning the router on, please press the Reset Button on the back of the modem, and hold the button until all the lights on the modem begin to flash and then it will reboot itself to restore the factory default settings. The login username and password will then be reset to admin. You can then access its GUI via its default IP address at <http://192.168.1.254/>.

#### **NOTE:**



Before the router is turned on to initiate its recovery process, please configure the IP address of the PC to 192.168.1.1 and then proceed with the following steps:

1. Turn off the router.
2. Turn on the router (the IP of the router will reset to an Emergency IP address, like 192.168.1.254).

# Cabling

One of the most common causes of problems is because of bad cabling or VDSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and VDSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analog modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your VDSL connection or may result in frequent disconnections.

# Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

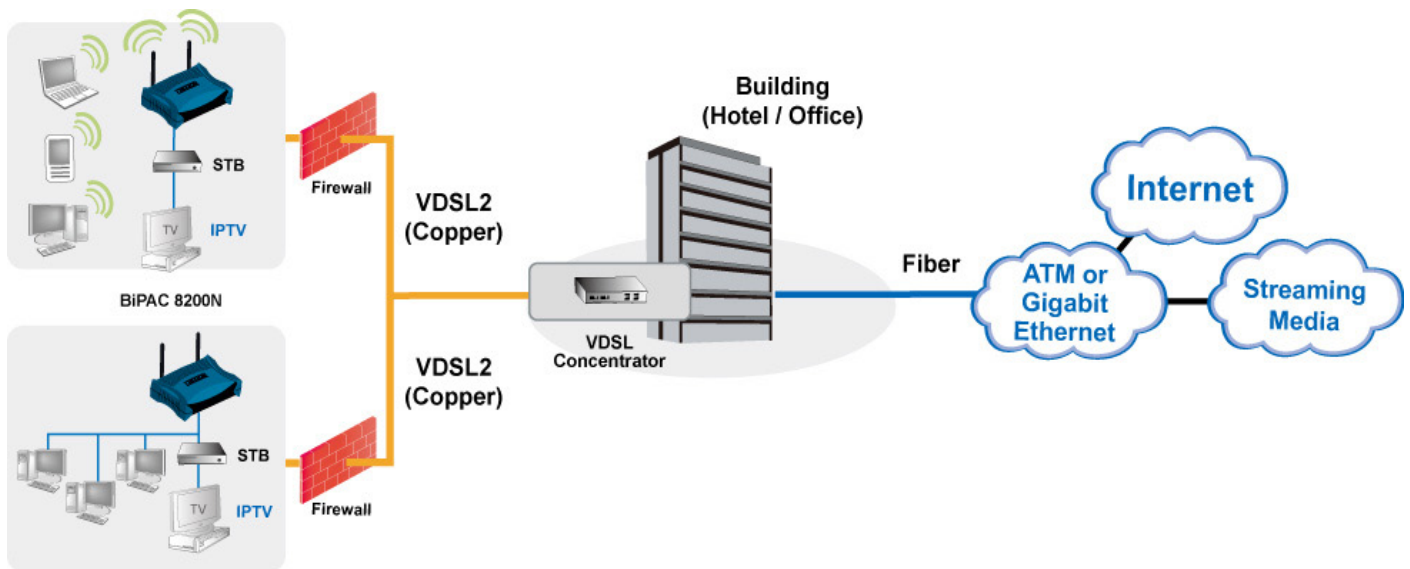
Please follow the following steps to configure your PC network environment.



Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

# Applications of the device

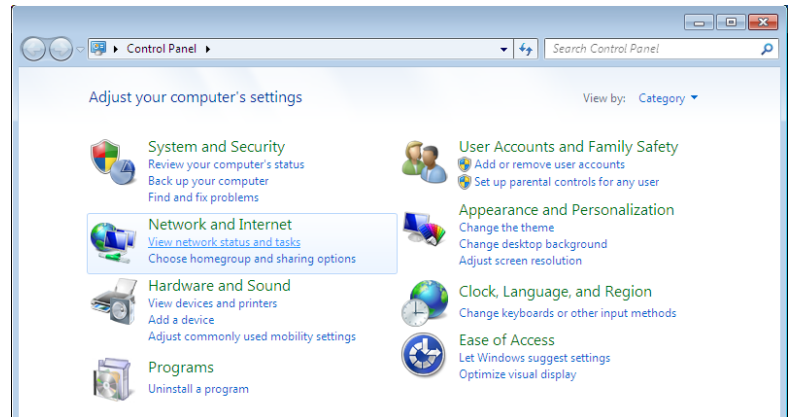
## Deployment scenario for VDSL using FTTx



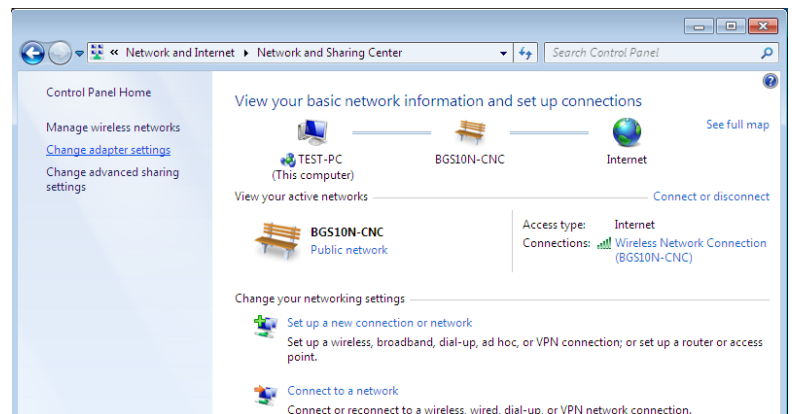
# Network Configuration

## Configuring PC in Windows 7

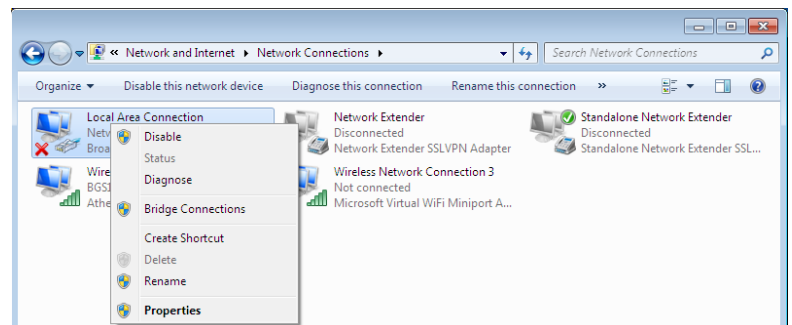
1. Go to Start. Click on Control Panel.
2. Then click on Network and Internet.



3. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

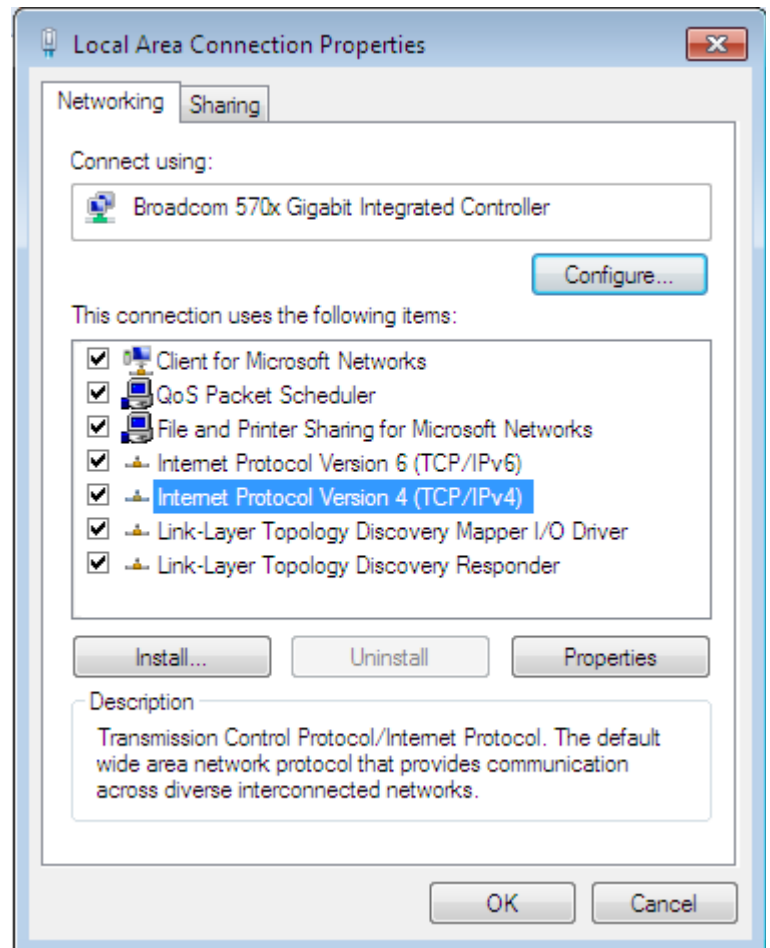


4. Select the Local Area Connection, and right click the icon to select Properties.

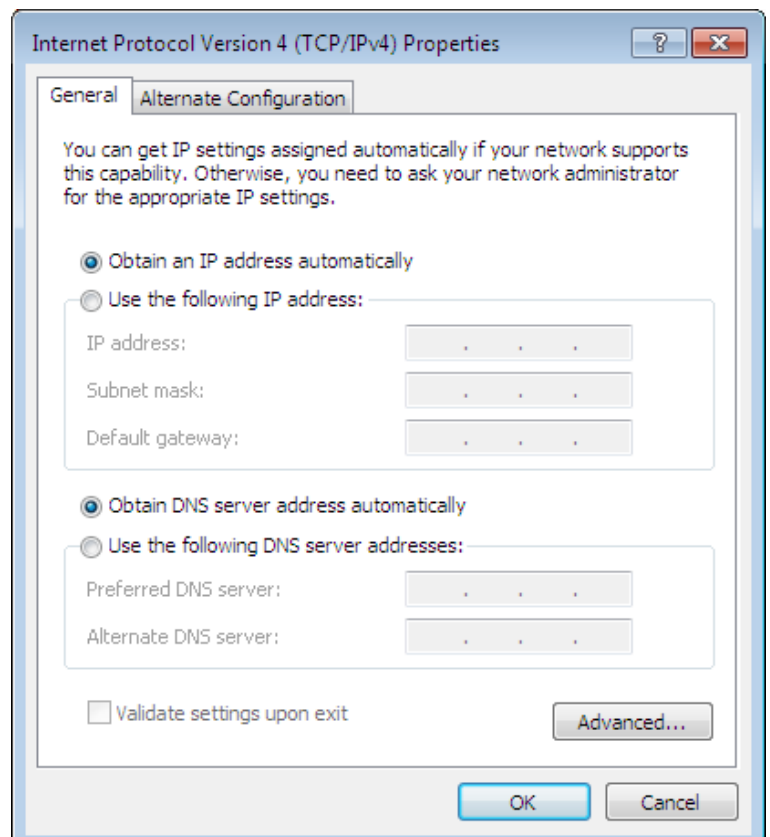




5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.

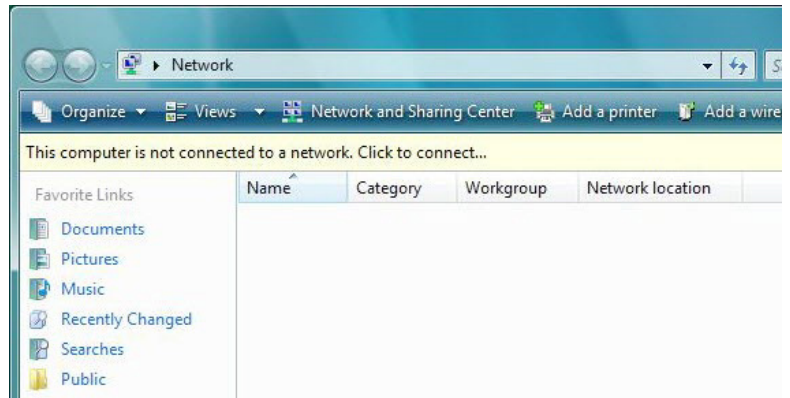


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



# Configuring PC in Windows Vista

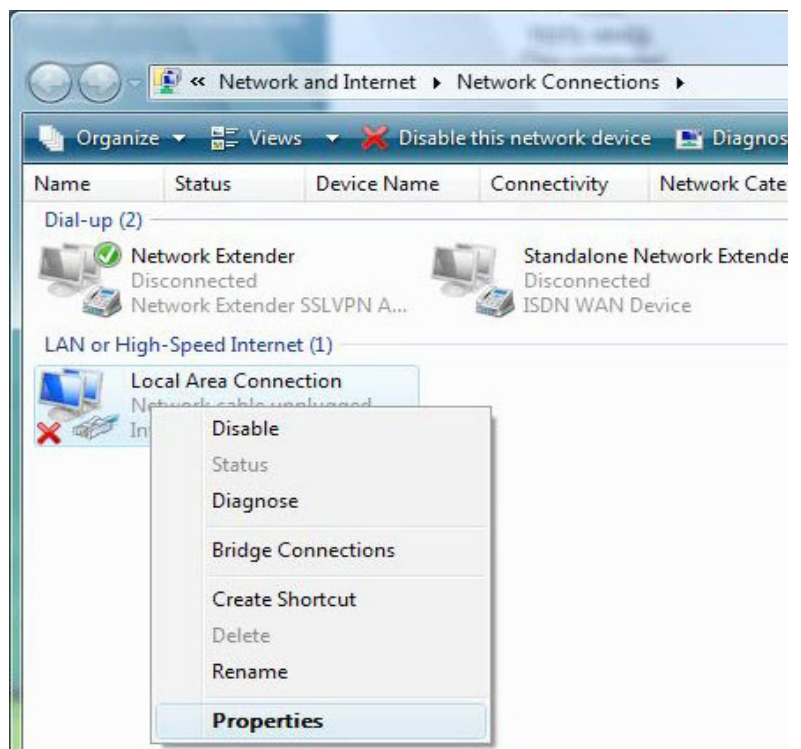
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



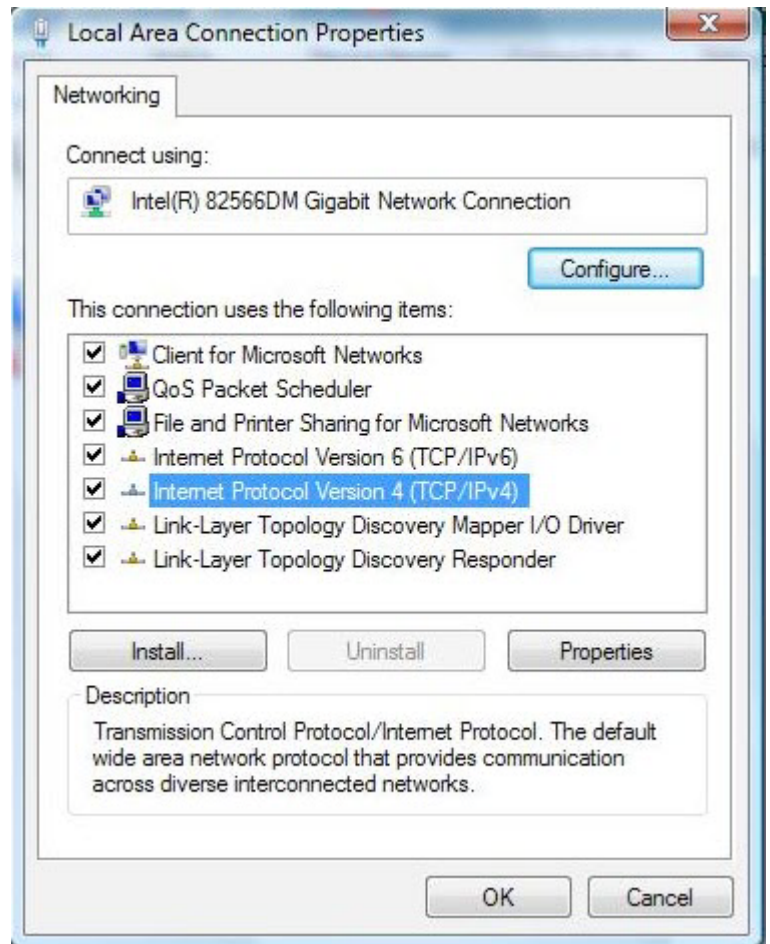
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



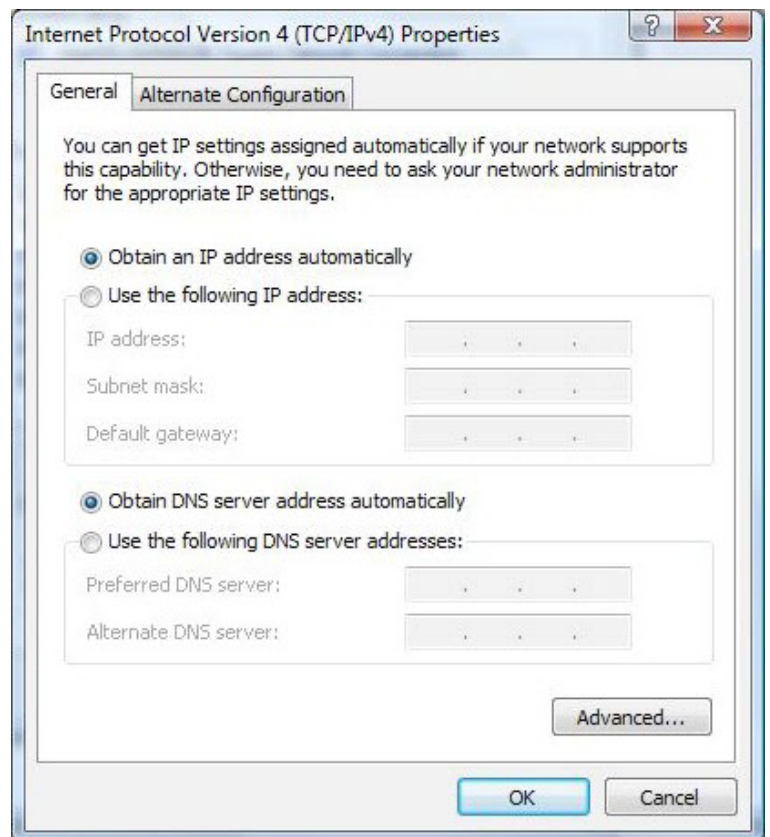
4. Select the Local Area Connection, and right click the icon to select Properties.



5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.

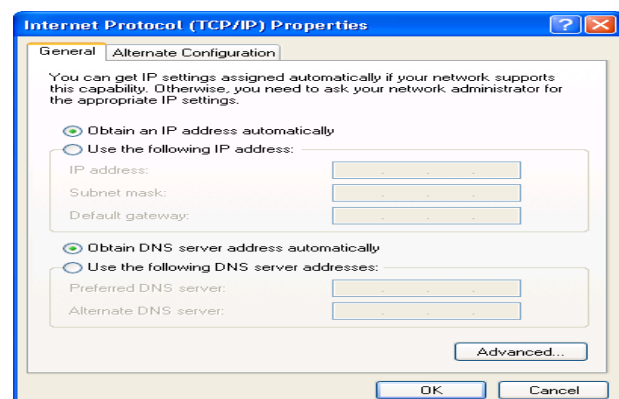
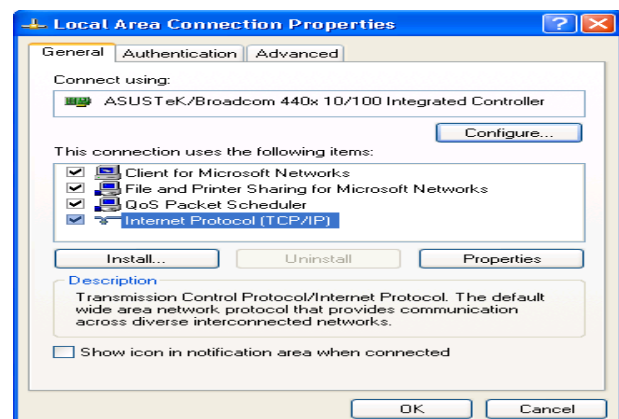
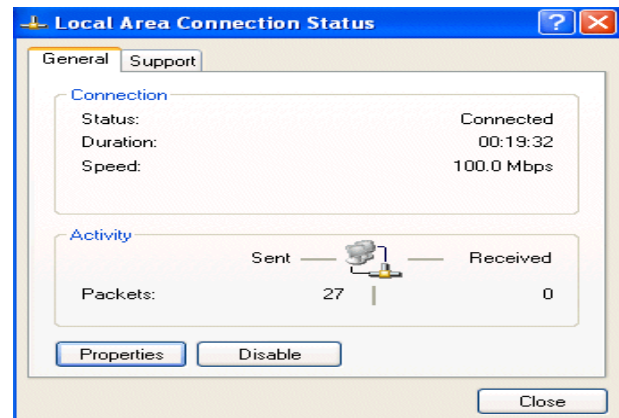
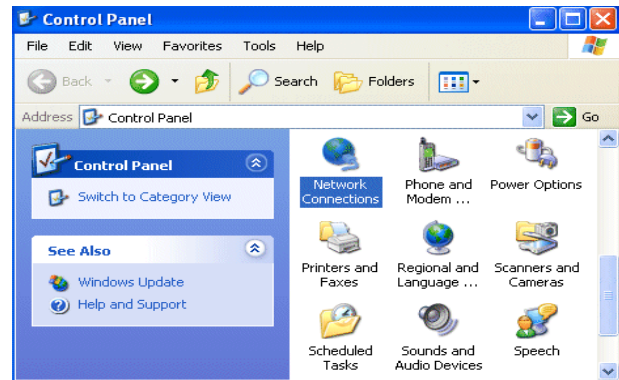


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



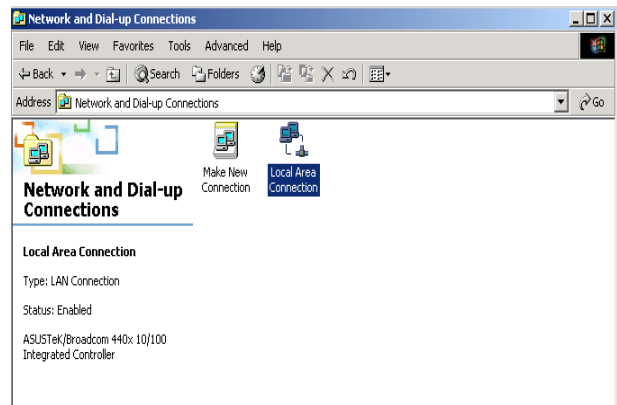
# Configuring PC in Windows XP

1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.
3. In the Local Area Connection Status window, click Properties.
4. Select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

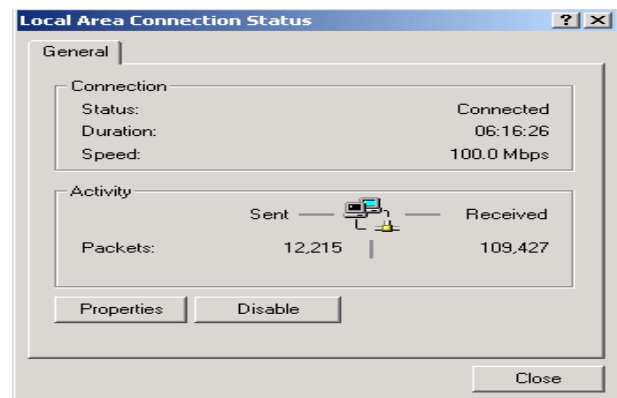


# Configuring PC in Windows 2000

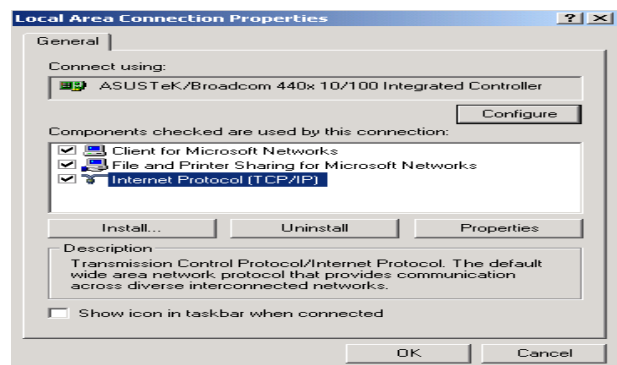
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



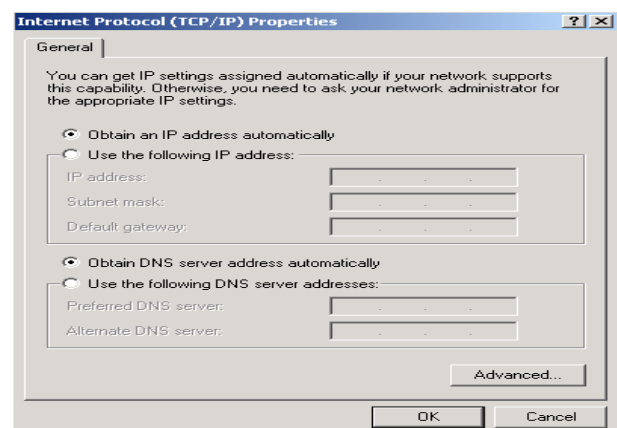
3. In the Local Area Connection Status window click Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.

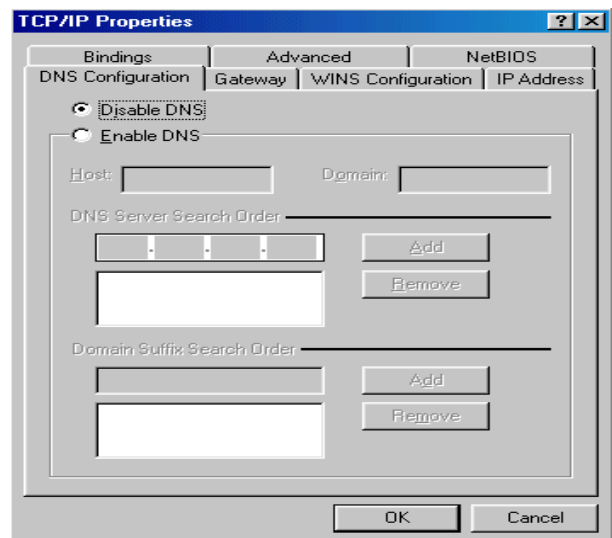
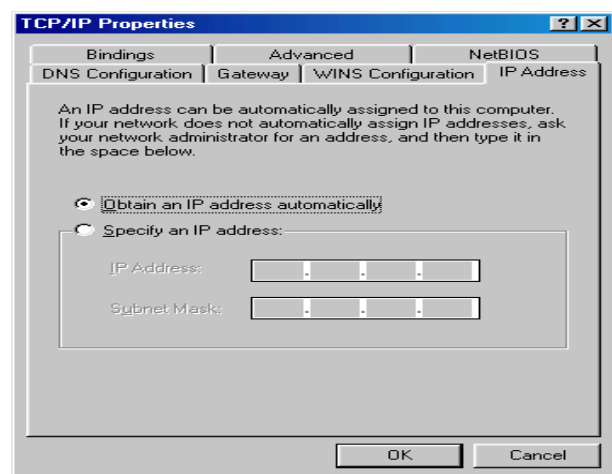
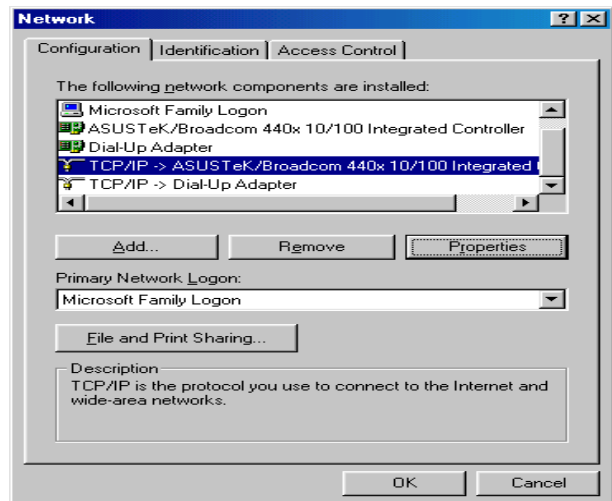


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.



# Configuring PC in Windows 95/98/Me

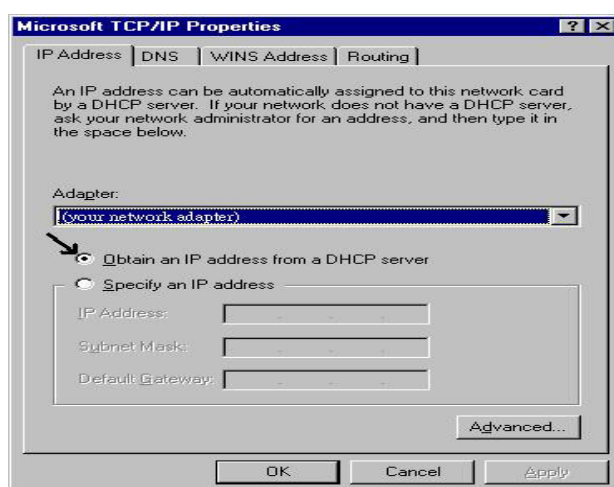
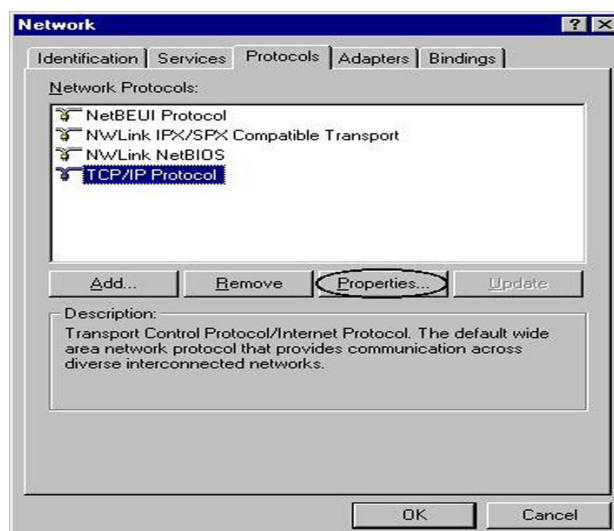
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.
3. Select the Obtain an IP address automatically radio button.
4. Then select the DNS Configuration tab.
5. Select the Disable DNS radio button and click OK to finish the configuration.





# Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.
3. Select the Obtain an IP address from a DHCP server radio button and click OK.



# Factory Default Settings

Before configuring your router, you need to know the following default settings.

## Web Interface (Username and Password)

▶ Username: admin

▶ Password: admin

The default username and password are “**admin**” and “**admin**” respectively.



### Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

## Device LAN IP settings

▶ IP Address: 192.168.1.254

▶ Subnet Mask: 255.255.255.0

## ISP setting in WAN site

▶ PPPoE

## DHCP server

▶ DHCP server is enabled.

▶ Start IP Address: 192.168.1.100

▶ IP pool counts: 100

## LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	



## Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as PPPoE, Obtain an IP Address Automatically (DHCP), Fixed IP Address (Static IP).

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
Obtain an IP Address Automatically	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
Fixed IP Address	IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

# Chapter 4: Configuration

To easily configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There are basically 2 ways to configure your router before you are able to connect to the internet: **Easy Sign-On** & **Web Interface**. Configuration of each method will be discussed in detail in the following sections.

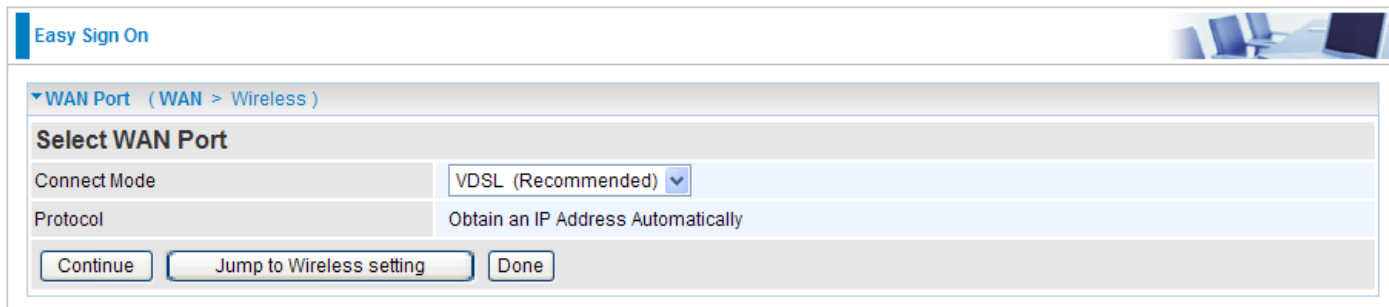
## Easy Sign-On (EZSO)

This special feature makes it easier for you to configure your router so that you can connect to the internet in a matter of seconds without having to logon to the router GUI for any detail configuration. This configuration method is usually auto initiated if user is to connect to the internet via Billion's router for the first time.

After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information that you have obtained from your ISP. By following the instructions given carefully and through the information you provide, the router will be configured in no time and you will find yourself surfing the internet sooner than you realize.

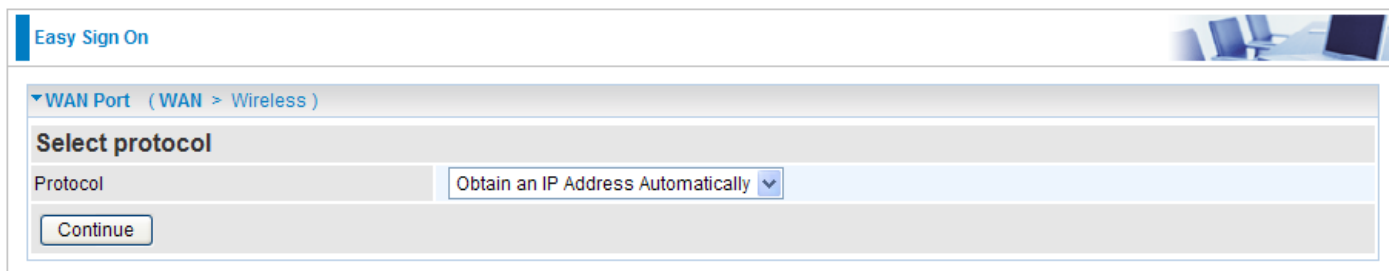
**Follow the Easy Sign-On configuration wizard to complete the basic network configuration.**

1. Connect your router with all the appropriate cables. Then, load your IE / netscape browser.
2. When the EZSO configuration wizard pops up, select the connect mode which you want to set up and then click continue. (There are two mode that you may select: one is "VDSL" and another is "EWAN".).



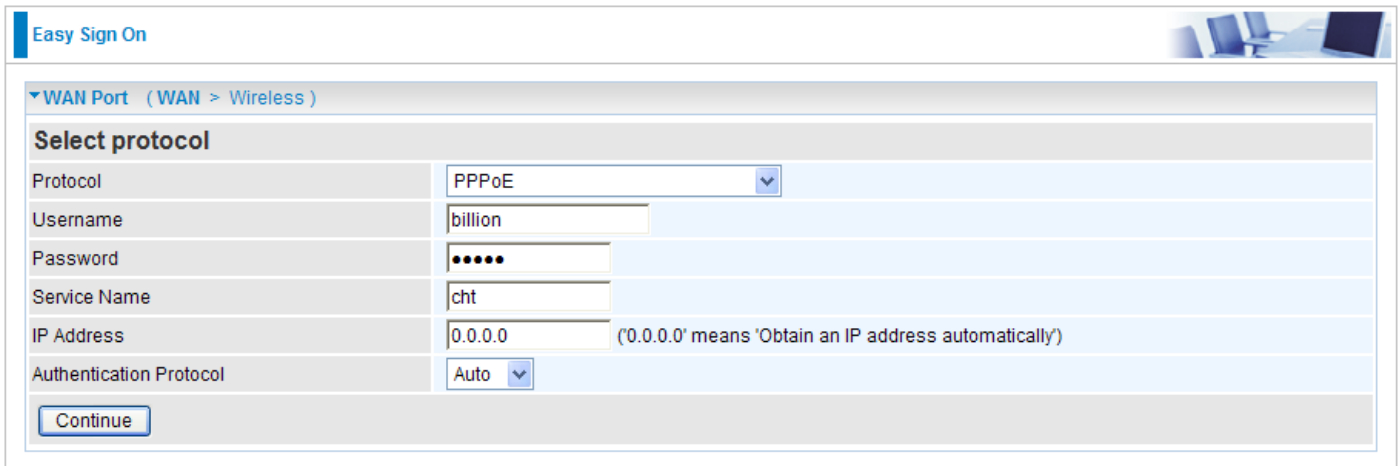
The screenshot shows the 'Easy Sign On' configuration wizard. At the top, there's a blue header with 'Easy Sign On' and a small image of a laptop. Below the header, a breadcrumb trail reads 'WAN Port (WAN > Wireless)'. The main section is titled 'Select WAN Port'. It contains two rows of settings: 'Connect Mode' with a dropdown menu set to 'VDSL (Recommended)', and 'Protocol' with a text field containing 'Obtain an IP Address Automatically'. At the bottom, there are three buttons: 'Continue', 'Jump to Wireless setting', and 'Done'.

3. Show Auto scan result - Protocol information.



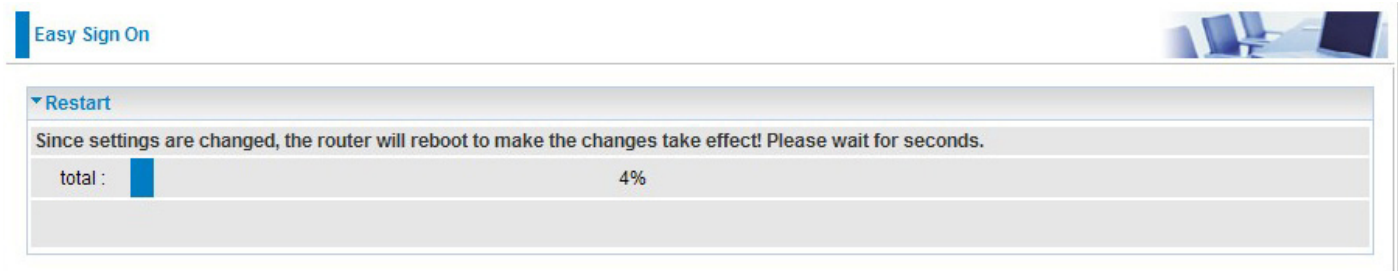
The screenshot shows the 'Easy Sign On' configuration wizard at the 'Select protocol' step. The breadcrumb trail is 'WAN Port (WAN > Wireless)'. The main section is titled 'Select protocol'. It contains one row of settings: 'Protocol' with a dropdown menu set to 'Obtain an IP Address Automatically'. At the bottom, there is a single 'Continue' button.

4. Please enter all the information in the blanks provided and then click Continue.




The screenshot shows the 'Easy Sign On' interface with a blue header bar. Below the header, there's a tab labeled 'WAN Port (WAN > Wireless)'. The main section is titled 'Select protocol' and contains a form with the following fields: 'Protocol' (dropdown menu set to 'PPPoE'), 'Username' (text box with 'billion'), 'Password' (password box with 6 dots), 'Service Name' (text box with 'cht'), 'IP Address' (text box with '0.0.0.0' and a note '(0.0.0.0 means 'Obtain an IP address automatically')'), and 'Authentication Protocol' (dropdown menu set to 'Auto'). At the bottom left of the form is a 'Continue' button.

5. The device will reboot and then load the new configuration.



The screenshot shows the 'Easy Sign On' interface with a blue header bar. Below the header, there's a tab labeled 'Restart'. The main section contains the text 'Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.' Below this text is a progress bar labeled 'total :'. The progress bar is a blue bar that is approximately 4% full, with '4%' written to its right.



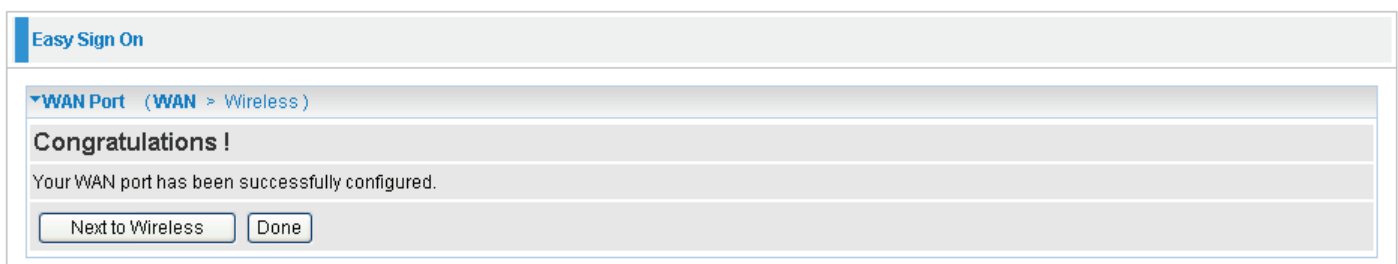
The screenshot shows the 'Easy Sign On' interface with a blue header bar. Below the header, there's a tab labeled 'WAN Port (WAN > Wireless)'. The main section contains the text 'Please wait while the device is configured.' Below this text is a large, empty rectangular box.

**Note: If any error occurs during device configuration that results in WAN connection failure, the system will prompt that the setup has failed.**



The screenshot shows the 'Easy Sign On' interface with a blue header bar. Below the header, there's a tab labeled 'WAN Port'. The main section contains a red 'Fail!!' message. Below the message is a text box that says 'WAN port setting is not successful (authentication fail), you can do this procedure again.'


6. If all information provided is valid and the device successfully connects to WAN, a dialog box will appear to signify the completion of the WAN port setup. At this point you can either click Done to finish the EZSO configuration or you can click Next to wireless to proceed to the wireless configuration if you have.



The screenshot shows the 'Easy Sign On' interface with a blue header bar. Below the header, there's a tab labeled 'WAN Port (WAN > Wireless)'. The main section is titled 'Congratulations !' and contains the text 'Your WAN port has been successfully configured.' Below this text are two buttons: 'Next to Wireless' and 'Done'.

7. Select Enable and enter the necessary information in the blanks provided for the Wireless LAN setting (wireless setting is only available for BiPAC 8200N) if you would like to use this feature and then click Continue.

Easy Sign On




▼ Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	<input type="text" value="wlan-ap"/>
Channel ID	<input type="text" value="Channel 1 (2.412 GHz)"/>
Security Mode	<input type="text" value="Disable"/>

Continue

Easy Sign On




▼ Save configuration

Saving configuration to FLASH. Please wait for 10 seconds

8. The system will save your new configuration and complete the setup. You can test the connection by clicking on the URL link provided. If the setup is successful you will be redirected to website.

Easy Sign On



▼ Process finished

**Success.**

The Easy-Sign-On process is finished. Your device has been successfully configured.

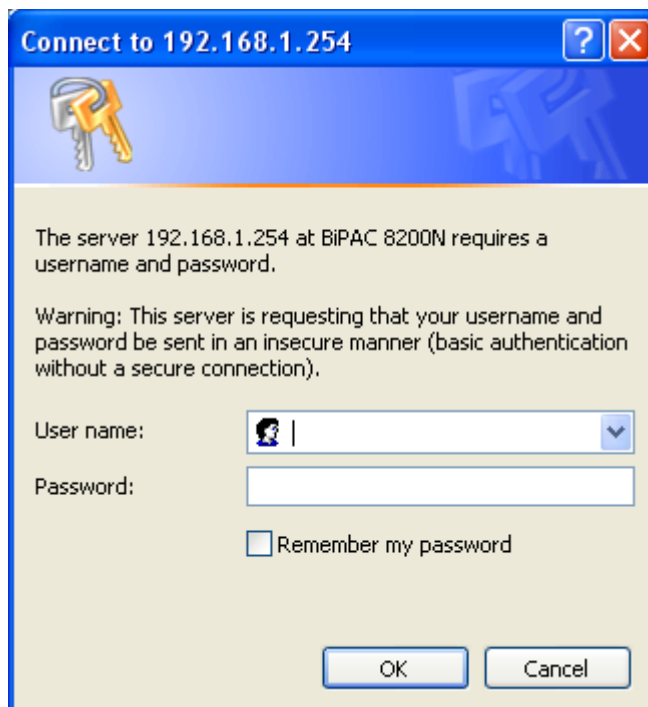
You can now:

1. Log onto the router management interface for more advanced settings on <http://192.168.1.254/>

2. Continue to [tw.yahoo.com/](http://tw.yahoo.com/)

## Configuration via Web Interface

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a login window prompt will appear. The default username and password are “admin” and “admin” respectively.

A Windows-style login dialog box titled "Connect to 192.168.1.254". It features a blue header bar with a question mark and close button. Below the header is a yellow background area with a key icon. The text inside says: "The server 192.168.1.254 at BiPAC 8200N requires a username and password." followed by a warning: "Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection)." There are two input fields: "User name:" with a dropdown arrow and "Password:" with a text box. Below the password field is a checkbox labeled "Remember my password". At the bottom are "OK" and "Cancel" buttons.

Connect to 192.168.1.254

The server 192.168.1.254 at BiPAC 8200N requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

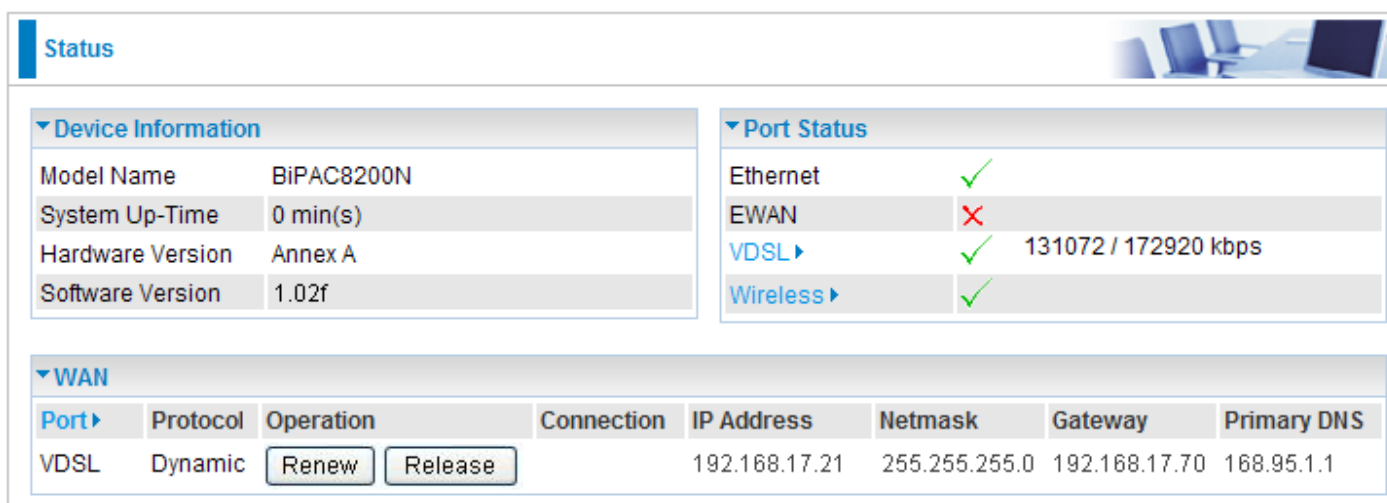
Password:

☐ Remember my password

OK Cancel

**Congratulations! You are now successfully logon to the Router!**

If the authentication succeeds, the homepage Status will appear on the screen.

The router's status page, titled "Status" in a blue bar. It contains three main sections: "Device Information", "Port Status", and "WAN".

Device Information	
Model Name	BiPAC8200N
System Up-Time	0 min(s)
Hardware Version	Annex A
Software Version	1.02f

Port Status	
Ethernet	✓
EWAN	✗
VDSL ▶	✓ 131072 / 172920 kbps
Wireless ▶	✓

WAN							
Port ▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
VDSL	Dynamic	<button>Renew</button> <button>Release</button>		192.168.17.21	255.255.255.0	192.168.17.70	168.95.1.1

# Quick Start

Whether on the Basic or Advanced Configuration Mode, click Quick Start link to WAN Port setup pages.

Step 1: This screen displays some information for WAN port. Select Connect Mode from the drop-down menu. There are 2 modes: VDSL and EWAN. Press Continue to go to the next configuration page.

## VDSL Mode

Quick Start

▼ WAN Port ( WAN > Wireless )

Select WAN Port

Connect Mode	VDSL (Recommended) ▼
Protocol	Obtain an IP Address Automatically

Continue

Jump to Wireless setting

**Connect mode:** VDSL

**Protocol:** Shows the current protocol in the device.

## EWAN Mode

Quick Start

▼ WAN Port ( WAN > Wireless )

Select WAN Port

Connect Mode	EWAN ▼
Protocol	PPPoE
Username	
IP Address	Obtain an IP Address Automatically

Continue

Jump to Wireless setting

**Connect mode:** EWAN

**Protocol:** Shows the current protocol in the device.

**Username:** Shows the current username.

**IP address:** Shows the current value of IP address in the device.

Step 2: Click on Continue to choose the Protocol to connect with EWAN or click Jump to Wireless Setting to use Protocol. There are 3 types of connection protocols available for WAN connect mode. **Each type of connection mode is described in the following sections of WAN Connect mode.**

Quick Start

▼ WAN Port ( WAN > Wireless )

Select protocol

Protocol	PPPoE	▼
Username	<input type="text"/>	
Password	<input type="password"/>	
Service Name	<input type="text"/>	
IP Address	0.0.0.0	('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto	▼

Continue

Step 3: After finishing configuring the WAN port connection, click Continue to proceed. The system will upload and apply the new WAN port configuration to the device.

Quick Start

▼ Restart

Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.

total :  12%

Quick Start

▼ WAN Port ( WAN > Wireless )

Please wait while the device is configured.

Quick Start

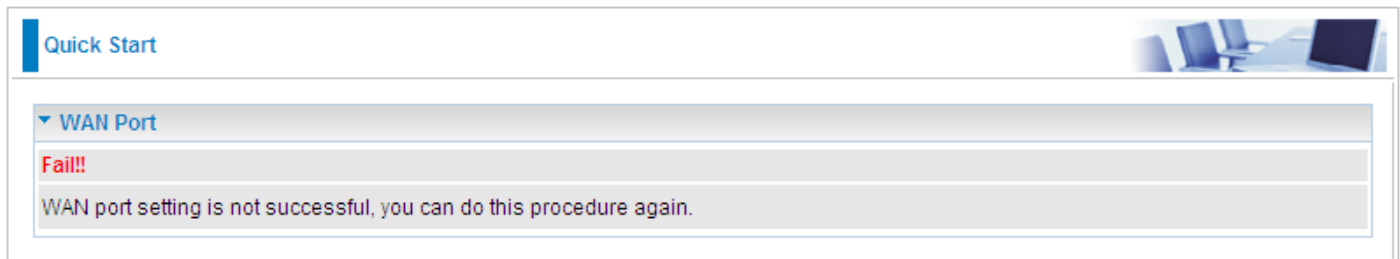
▼ WAN Port ( WAN > Wireless )

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless

**Note: If the WAN line is not ready, a page will display as below and your new configuration can not be saved.**



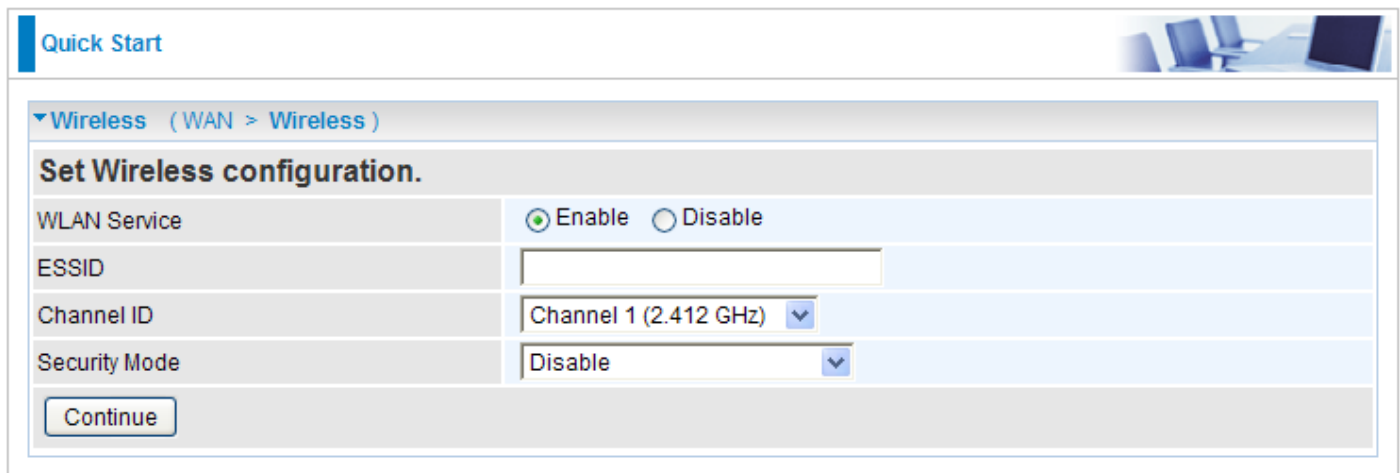
Quick Start

▼ WAN Port

**Fail!!!**

WAN port setting is not successful, you can do this procedure again.

Step 4: After the configuration is successful, click Next to Weireless button and you may proceed to configure the Wireless setting. There are 4 types of security mode: WPA, WPA2, WPA/ WPA2 Pre-Shared Key and WEP. Please refer to the **Wireless Setting Mode** section for detail description of each security mode.



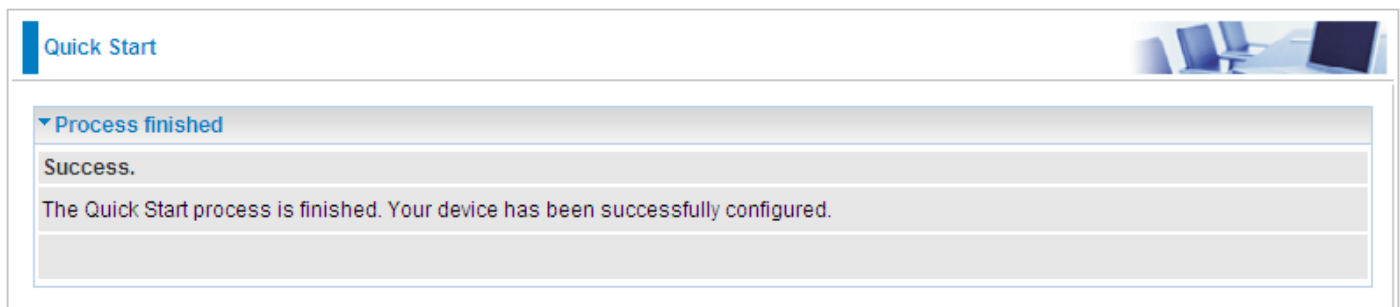
Quick Start

▼ Wireless ( WAN > Wireless )

**Set Wireless configuration.**

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	<input type="text"/>
Channel ID	Channel 1 (2.412 GHz) ▼
Security Mode	Disable ▼

Step 5: After finishing configuring the WLAN setting, press Continue to finish the QuickStart.



Quick Start

▼ Process finished

**Success.**

The Quick Start process is finished. Your device has been successfully configured.



## WAN Connect Mode

There are 4 types of wireless connect modes: **Obtain an IP Address Automatically**, **Fixed IP Address**, **PPPoE connection** and **Pure Bridge**.

### Obtain an IP Address Automatically

When connecting to the ISP, your router also functions as a DHCP client. The device can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.

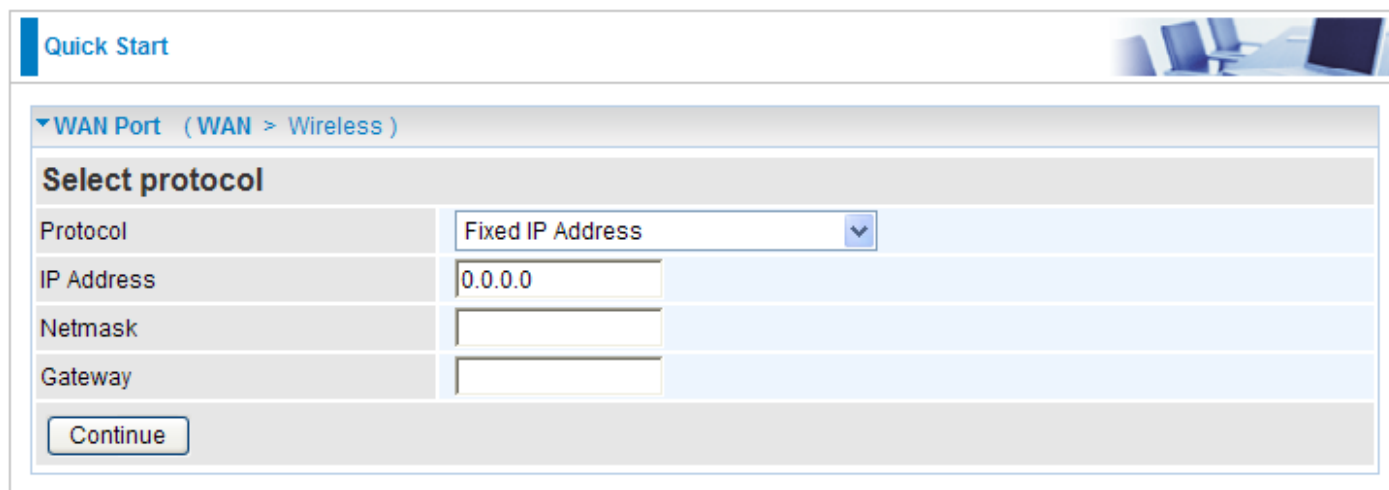
Select this protocol enables the device to automatically retrieve IP address.



The screenshot shows the 'Quick Start' section of the WAN Port configuration page. The breadcrumb trail is 'WAN > Wireless'. Under the 'Select protocol' heading, the 'Protocol' dropdown menu is set to 'Obtain an IP Address Automatically'. A 'Continue' button is located at the bottom left of the configuration area.

### Fixed IP Address

Select this option to set static IP information. You will need to enter the information provided to you by your ISP.



The screenshot shows the 'Quick Start' section of the WAN Port configuration page. The breadcrumb trail is 'WAN > Wireless'. Under the 'Select protocol' heading, the 'Protocol' dropdown menu is set to 'Fixed IP Address'. Below this, there are three input fields: 'IP Address' (containing '0.0.0.0'), 'Netmask', and 'Gateway'. A 'Continue' button is located at the bottom left of the configuration area.

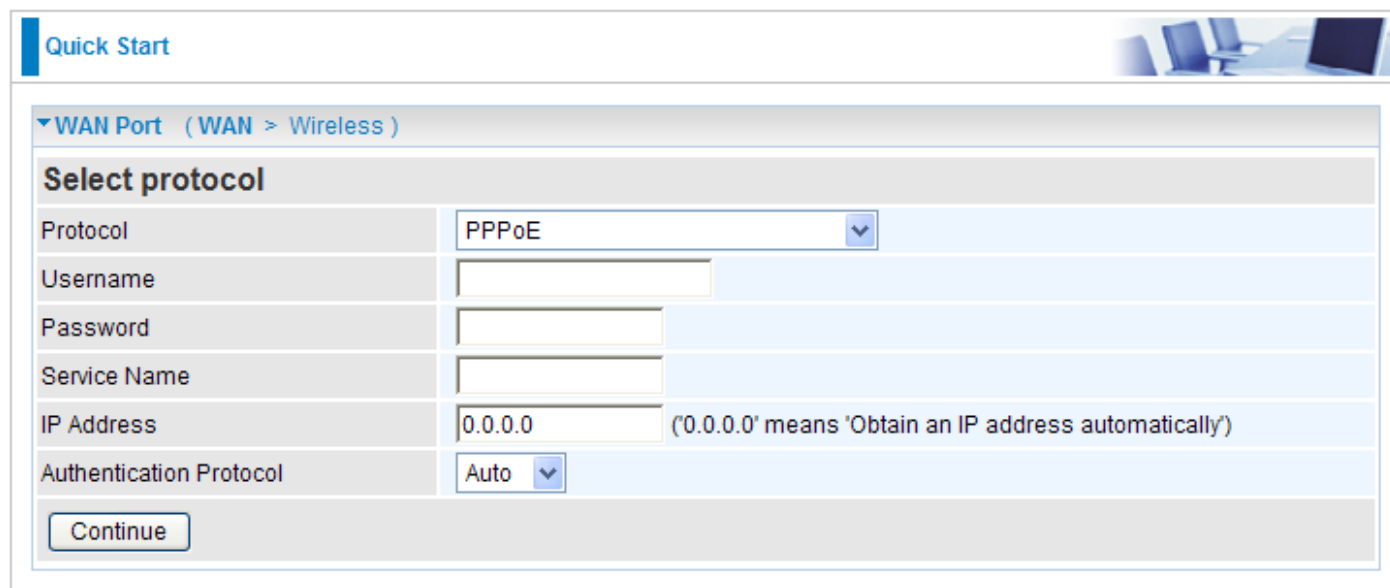
**IP Address:** Enter your fixed IP address. Each IP address entered must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

**Netmask:** User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

**Gateway:** Enter the IP address of the default gateway.

## PPPoE

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



The screenshot shows a web-based configuration interface for a network device. At the top, there is a 'Quick Start' tab and a breadcrumb trail '( WAN > Wireless )'. Below this, a section titled 'Select protocol' contains a form with the following fields: 'Protocol' (set to 'PPPoE'), 'Username' (empty), 'Password' (empty), 'Service Name' (empty), 'IP Address' (set to '0.0.0.0' with a note '(0.0.0.0) means 'Obtain an IP address automatically''), and 'Authentication Protocol' (set to 'Auto'). A 'Continue' button is located at the bottom of the form.

**Username:** Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is the format of username “username@ispname” instead of “username”.

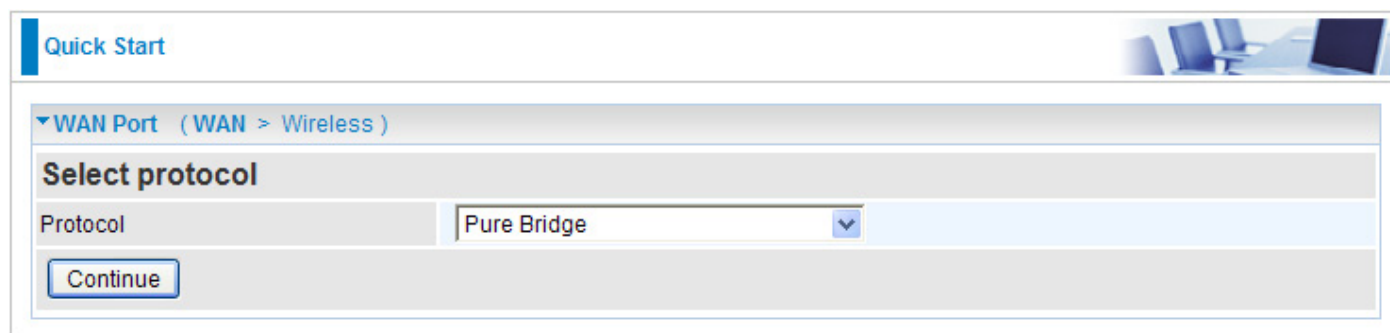
**Password:** Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

**Service Name:** This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

**IP Address:** Enter your fixed IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

**Authentication Protocol:** Default is Auto. Please consult your ISP on whether to use Pap or Chap.

## Pure Bridge



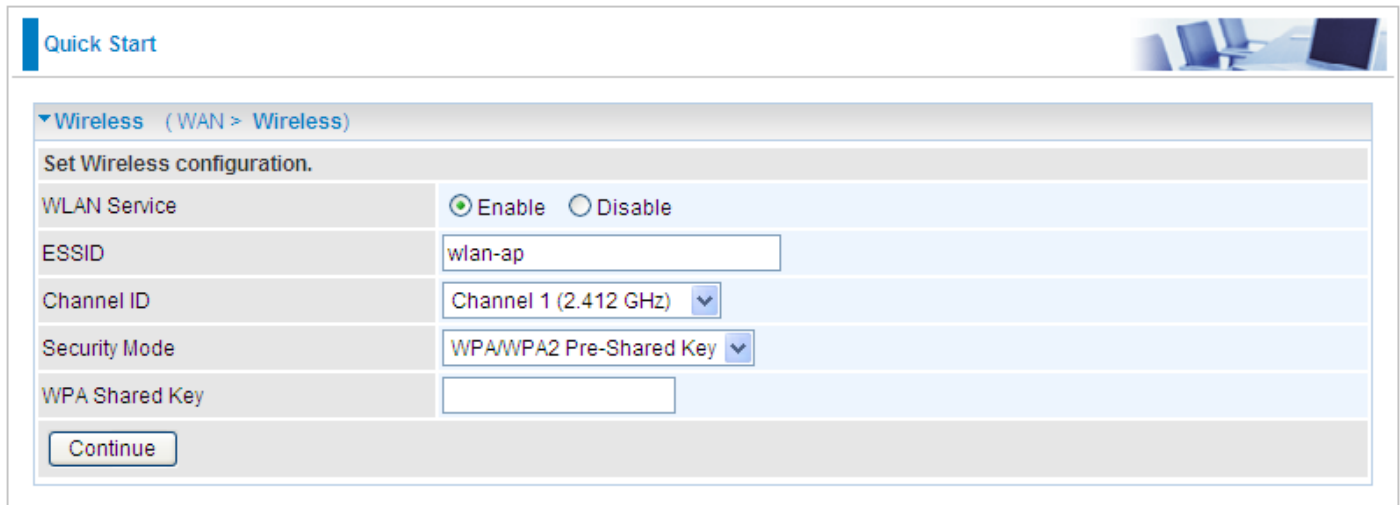
The screenshot shows a web-based configuration interface for a network device. At the top, there is a 'Quick Start' tab and a breadcrumb trail '( WAN > Wireless )'. Below this, a section titled 'Select protocol' contains a form with the following fields: 'Protocol' (set to 'Pure Bridge') and a 'Continue' button.

## Wireless Setting Mode

There are 4 types of wireless security modes: [WPA Pre-Shared Key](#), [WPA2 Pre-Shared Key](#), [WPA/WPA2 Pre-Shared Key](#) and [WEP](#).

### WPA / WPA2 / WPA/WPA2 Pre-Shared Key

WPA and WPA2 pre-shared keys are an authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.



Quick Start

▼ Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	<input type="text" value="wlan-ap"/>
Channel ID	<input type="text" value="Channel 1 (2.412 GHz)"/>
Security Mode	<input type="text" value="WPA/WPA2 Pre-Shared Key"/>
WPA Shared Key	<input type="text"/>

**WLAN Service:** Default setting is Enable. If you want to use wireless, you can select Enable.

**ESSID:** The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

**Channel ID:** Select the channel ID that you would like to use.

**Security Mode:** You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is Disable.

**WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Quick Start

Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service

☒ Enable
 ☐ Disable

ESSID

wlan-ap

Channel ID

Channel 1 (2.412 GHz)

Security Mode

WEP

Default Used WEP Key

☒ 1
 ☐ 2
 ☐ 3
 ☐ 4

Key

WEP 64 - Hex: 10 Hex codes, (0~9, a~f, A~F). EX: 11aa22cc33.

WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.

WEP 128 - Hex: 26 Hex codes, (0~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.

WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?l dbd3ert.

Continue

**WLAN Service:** Default setting is set to Enable. If you want to use wireless, you can select Enable.

**ESSID:** The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

**Channel ID:** Select the channel ID that you would like to use.

**Security Mode:** You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is Disable.

**Default Used WEP Key:** Select the encryption key ID; please refer to **Key (1~4)** below.

**Key (1-4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can either be HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

# Basic Configuration Mode

## Status

### Device Information

Status

▼ Device Information

Model Name	BiPAC8200N
System Up-Time	0 min(s)
Hardware Version	Annex A
Software Version	1.02f

▼ Port Status

Ethernet	✓
EWAN	✗
VDSL ▶	✓ 131072 / 172920 kbps
Wireless ▶	✓

▼ WAN

Port ▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
VDSL	Dynamic	<input type="button" value="Renew"/> <input type="button" value="Release"/>		192.168.17.21	255.255.255.0	192.168.17.70	168.95.1.1

**Model Name:** Provide a name for the router for identification purposes.

**System Up-Time:** Record system up-time.

**Hardware Version:** Device version.

**Software Version:** Firmware version.

### Port Status

**Port Status:** User can look up to see if they are connected to Ethernet, EWAN, VDSL and Wireless. You are allowed to click Wireless link to go to Wireless Parameters configuration screen.

### WAN

**Port:** Name of the WAN connection. You are allowed to click this link to go to WAN Connection configuration screen.

**Protocol:** The current protocol in the device.

**Operation:** Current status in WAN interface.

**Connection:** Current connection status.

**IP Address:** WAN port IP address.

**Netmask:** WAN port IP subnet mask.

**Gateway:** IP address of the default gateway.

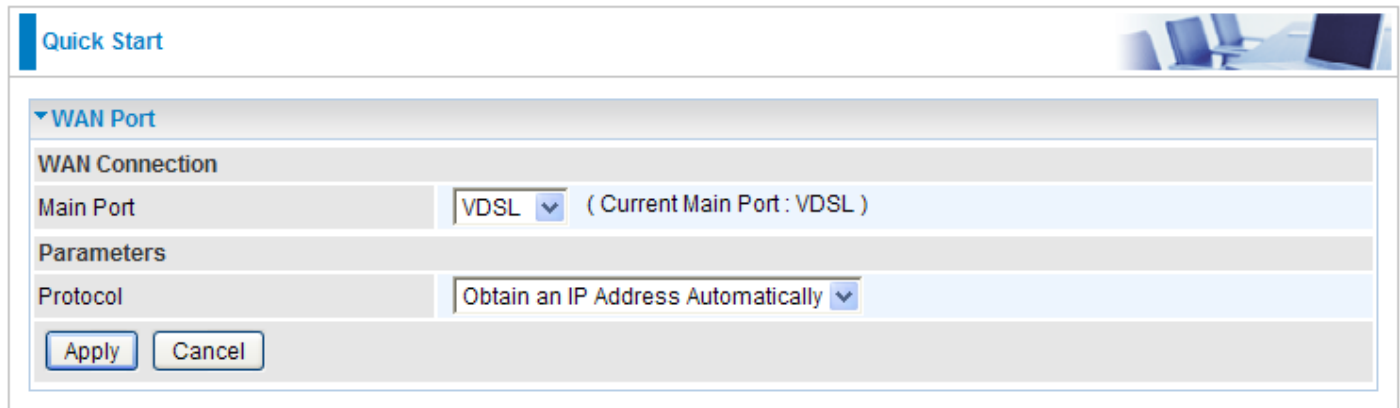
**Primary DNS:** IP address of the primary DNS server.

## WAN – Main Port: VDSL

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

### Obtain IP Address Automatically (VDSL)

By configuring these settings, the device is able to obtain IP settings automatically from the ISP.




The screenshot shows a web-based configuration interface for a device. At the top left, there is a 'Quick Start' link. The main content area is titled 'WAN Port' and contains two sections: 'WAN Connection' and 'Parameters'. In the 'WAN Connection' section, the 'Main Port' is set to 'VDSL' with a dropdown arrow, and a note indicates '( Current Main Port : VDSL )'. In the 'Parameters' section, the 'Protocol' is set to 'Obtain an IP Address Automatically' with a dropdown arrow. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

**Protocol:** Select the protocol you will use in the device.

Click Apply to confirm the settings.

## Fixed IP Address (VDSL)

A Static WAN connection will be configured according to the IP properties defined by your ISP.

**Quick Start**

**▼ WAN Port**

**WAN Connection**

**Main Port** VDSL ▼ ( Current Main Port : VDSL )

**Parameters**

**Protocol** Fixed IP Address ▼

**IP Address**

**Netmask**

**Gateway**

**Protocol:** Select the protocol you will use in the device.

**IP Address:** Enter your fixed IP address.

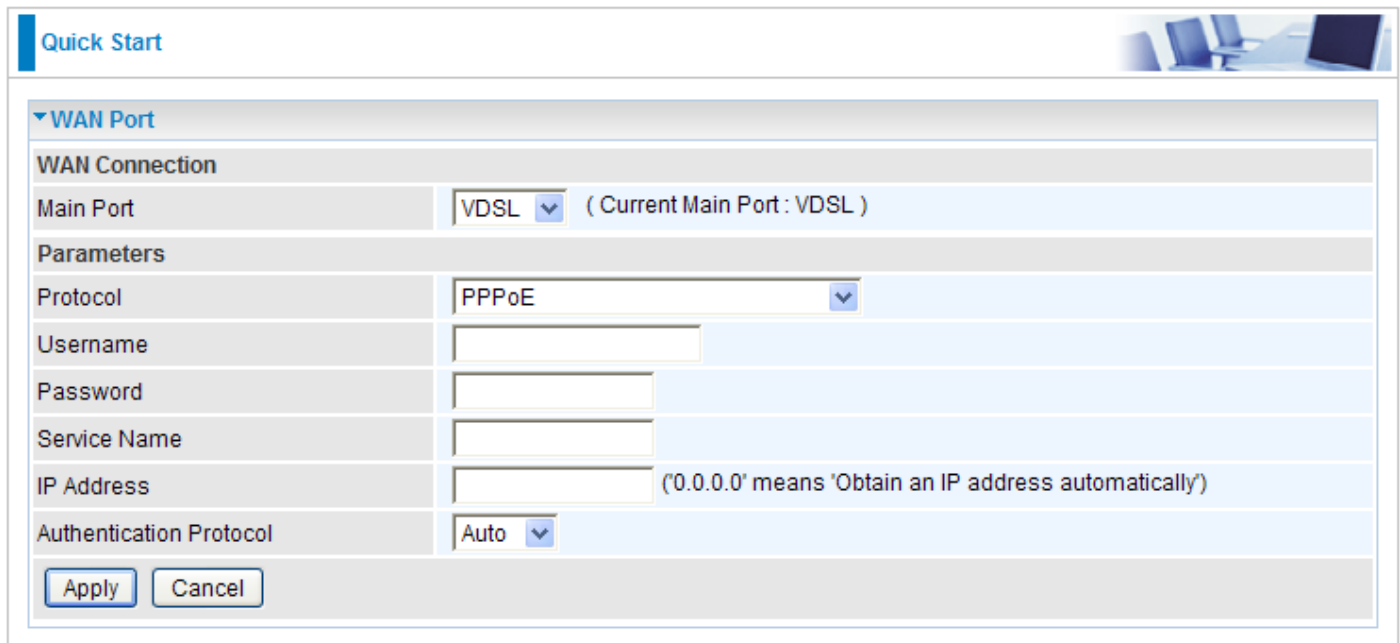
**Netmask:** User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

**Gateway:** Enter the IP address of the default gateway (if given).

Click Apply to confirm the settings.

## PPPoE Connection (VDSL)

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



The screenshot shows a 'Quick Start' window for configuring a WAN Port. The 'WAN Port' section is expanded, showing 'WAN Connection' with 'Main Port' set to 'VDSL' (Current Main Port: VDSL). Under 'Parameters', 'Protocol' is set to 'PPPoE'. There are input fields for 'Username', 'Password', and 'Service Name'. The 'IP Address' field is empty, with a note '(0.0.0.0 means Obtain an IP address automatically)'. The 'Authentication Protocol' is set to 'Auto'. At the bottom are 'Apply' and 'Cancel' buttons.

WAN Port	
WAN Connection	
Main Port	VDSL (Current Main Port: VDSL)
Parameters	
Protocol	PPPoE
Username	
Password	
Service Name	
IP Address	(0.0.0.0 means Obtain an IP address automatically)
Authentication Protocol	Auto
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Protocol:** Select the protocol you will use in the device.

**Username:** Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

**Password:** Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

**Service Name:** This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.


**IP Address:** Enter your WAN IP address. Leave the IP address empty or enter 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

**Authentication Protocol:** Default is Auto. Please consult your ISP on whether to use Pap and Chap.

Click Apply to confirm the settings.



## Pure Bridge (VDSL)

**Quick Start**

**▼ WAN Port**

**WAN Connection**

**Main Port** VDSL ( Current Main Port : VDSL )

**Parameters**

**Protocol** Pure Bridge

**Protocol:** Select the protocol you will use in the device.

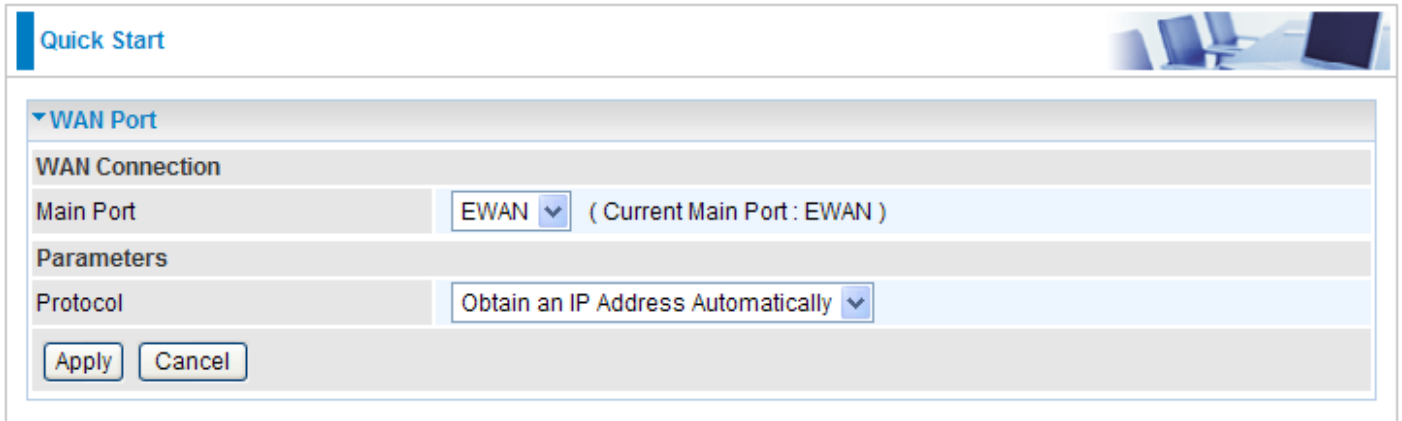
Click Apply to confirm the change.

## WAN – Main Port: EWAN

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

### Obtain IP Address Automatically (EWAN)

By configuring these settings, the device is able to obtain IP settings automatically from the ISP.




The screenshot shows a web-based configuration interface for a device. At the top left, there is a 'Quick Start' link. The main section is titled 'WAN Port' and contains two sub-sections: 'WAN Connection' and 'Parameters'. Under 'WAN Connection', the 'Main Port' is set to 'EWAN' with a dropdown arrow, and a note indicates '( Current Main Port : EWAN )'. Under 'Parameters', the 'Protocol' is set to 'Obtain an IP Address Automatically' with a dropdown arrow. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

**Protocol:** Select the protocol you will use in the device.

Click Apply to confirm the settings.

## Fixed IP Address (EWAN)

A Static WAN connection will be configured according to the IP properties defined by your ISP.

**Quick Start**

**▼ WAN Port**

**WAN Connection**

Main Port

EWAN ▼ ( Current Main Port : EWAN )

**Parameters**

Protocol

Fixed IP Address ▼

IP Address

0.0.0.0

Netmask

Gateway

Apply

Cancel

**Protocol:** Select the protocol you will use in the device.

**IP Address:** Enter your fixed IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

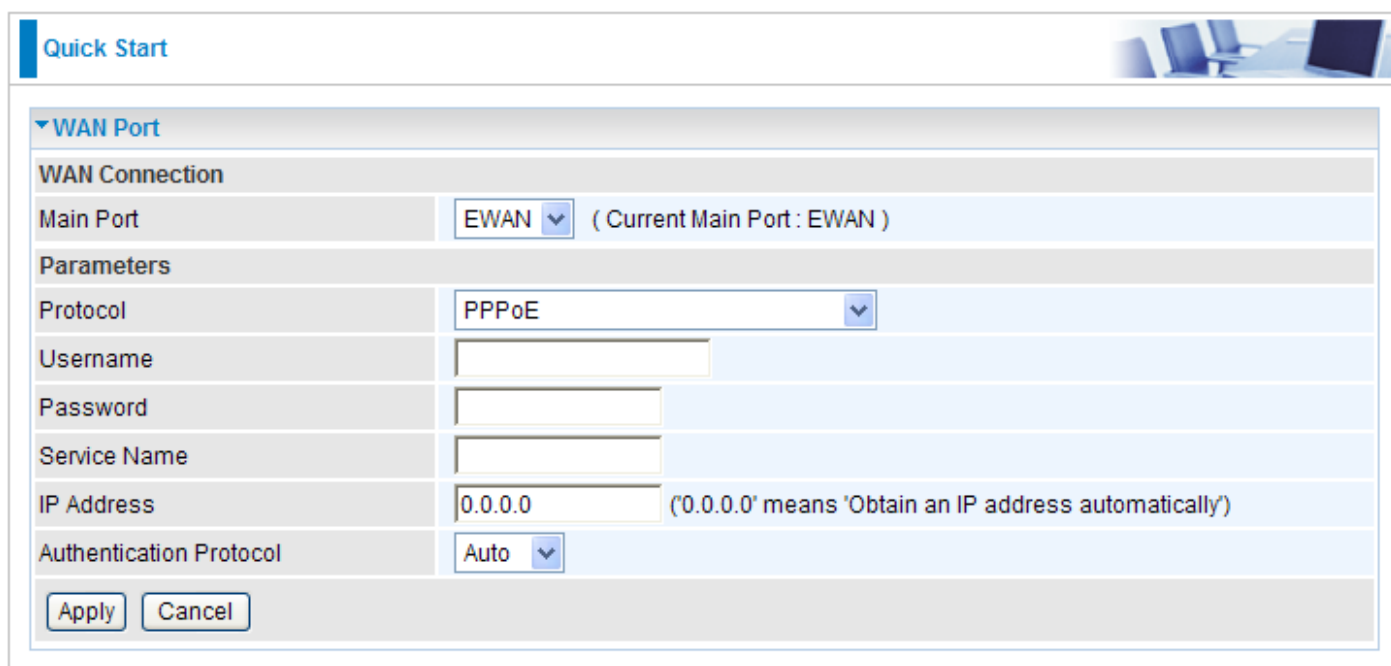
**Netmask:** User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

**Gateway:** Enter the IP address of the default gateway (if given).

Click Apply to confirm the settings.

## PPPoE Connection (EWAN)

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



**Quick Start**

**WAN Port**

**WAN Connection**

Main Port: EWAN ( Current Main Port : EWAN )

**Parameters**

Protocol: PPPoE

Username:

Password:

Service Name:

IP Address: 0.0.0.0 ("0.0.0.0" means 'Obtain an IP address automatically')

Authentication Protocol: Auto

Apply Cancel

**Protocol:** Select the protocol you will use in the device.

**Username:** Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

**Password:** Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

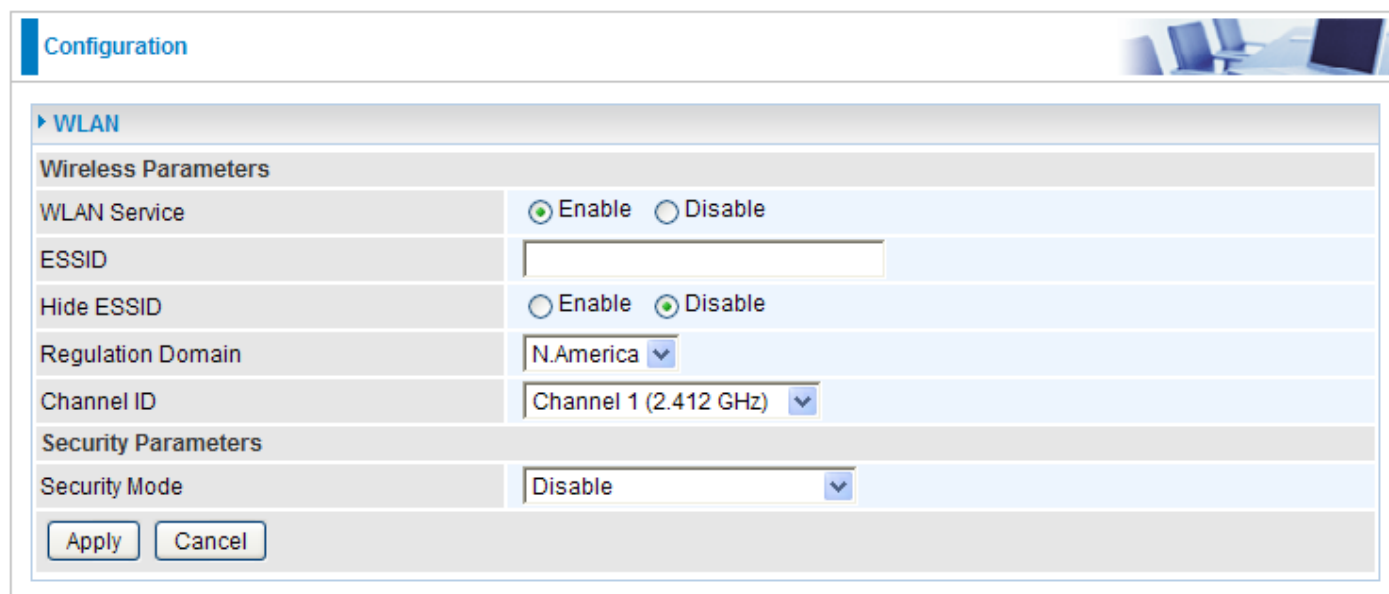
**Service Name:** This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

**IP Address:** Enter your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

**Auth. Protocol:** Default is Auto. Please consult your ISP on whether to use Pap and Chap.

Click Apply to confirm the settings.

# WLAN



**Configuration**

► **WLAN**

**Wireless Parameters**

WLAN Service: ☒ Enable ☐ Disable

ESSID:

Hide ESSID: ☐ Enable ☒ Disable

Regulation Domain: N.America ▼

Channel ID: Channel 1 (2.412 GHz) ▼

**Security Parameters**

Security Mode: Disable ▼

Apply Cancel

## Wireless Parameters

**WLAN Service:** Default setting is set to Enable. If you do not have any wireless, select Disable.

**ESSID:** The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change the default wlan-ap to a unique ID name that is already built into the router wireless interface. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

**Note:** *It is case sensitive and must not exceed 32 characters.*

**Hide ESSID:** It is used to broadcast its ESSID on the network so that when a wireless client searches for a network, the router can be discovered and recognized. Default setting is Disable.

**Enable:** When enabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.

**Disable:** When disabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

**Regulation Domain:** There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

**Channel ID:** Select the wireless connection channel ID that you would like to use.

**Note:** *Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).*

## Security Parameters

**Security Mode:** You can disable or enable the function with WPA or WEP to protect the wireless network. The default mode of wireless security is Disable.

Click Apply to confirm the settings.

## Security Mode

### WPA / WPA2 / WPA/WPA2 Pre-Shared Key

Security Parameters	
Security Mode	WPA/WPA2 Pre-Shared Key ▼
WPA Shared Key	<input type="text"/>
Group Key Renewal	3600 seconds

**Security Mode:** You can disable or enable with WPA or WEP for protecting wireless network.

**WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

**Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

### WEP

Security Parameters	
Security Mode	WEP ▼
WEP Authentication	Shared Key ▼
Default Used WEP Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Passphrase (Generate Key)	<input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/>
Key 1	Hex ▼ <input type="text"/>
Key 2	Hex ▼ <input type="text"/>
Key 3	Hex ▼ <input type="text"/>
Key 4	Hex ▼ <input type="text"/>

WEP 64 - Hex: 10 Hex codes, (0~9, a~f, A~F). EX: 11aa22cc33.  
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.  
WEP 128 - Hex: 26 Hex codes, (0~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.  
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

**Security Mode:** You can disable or enable with WPA or WEP for protecting wireless network.

**WEP Authentication:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are 3 options to select from: **Open System**, **Share Key** and **Both**.

**Default Used WEP Key:** Select the encryption key ID; please refer to **Key (1~4)** below.

**Passphrase:** This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

**Key (1-4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 or 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

# Advanced Configuration Mode

## Status

Status

▼ Device Information

Model Name	BIPAC8200N
Host Name ▶	home.gateway
System Up-Time	0 min(s)
Current Time ▶	Sat Jan 1 00:00:56 2000
Hardware Version	Annex A
Software Version	1.02f
MAC Address	00:1e:ab:b0:00:00

▼ Port Status

Ethernet	✓	
EWAN	✗	
VDSL ▶	✓	131072 / 172920 kbps
Wireless ▶	✓	

▼ WAN

Port ▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
VDSL	Dynamic	<input type="button" value="Renew"/> <input type="button" value="Release"/>		192.168.17.21	255.255.255.0	192.168.17.70	168.95.1.1

### Device Information

**Model Name:** Displays the model name.

**Host Name:** Provide a name for the router for identification purposes. Host Name lets you change the router name.

**System Up-Time:** Records system up-time.

**Current Time:** Set the current time. See the Time Zone section for more information.

**Hardware Version:** Device version.

**Software Version:** Firmware version.

**MAC Address:** The LAN MAC address.

### Port Status

**Port Status:** User can look up to see if they are connected to Ethernet, EWAN, VDSL and Wireless. You are allowed to click VDSL and Wireless link to go to VDSL Status screen or Wireless Parameters configuration screen.

### WAN

**Port:** Name of the WAN connection.

**Protocol:** The current protocol in the device.

**Operation:** The current status in WAN interface.

**Connection:** The current connection status.

**IP Address:** WAN port IP address.

**Netmask:** WAN port IP subnet mask.

**Gateway:** The IP address of the default gateway.

**Primary DNS:** The IP address of the primary DNS server.



## VDSL Status

VDSL (Very High Bitrate DSL) is a DSL technology providing faster data transmission. It can achieve incredible speeds and provides a complete home-communications/entertainment package.

This table displays all the information for VDSL connection.

Status		
▼ VDSL Status		
Parameters		
DSP Firmware Version	010100	
DMT Status	Up	
Electrical Length	0.6 dB	
	Upstream	Downstream
BAND ID	1	2
Line Attenuation	0.0 dB	0.0 dB
Signal Attenuation	0.0 dB	0.0 dB
Line Rate	128912 kbps	172920 kbps
Actual Data Rate	100052 kbps	100061 kbps
Attainable Rate	115419 kbps	191815 kbps
SNR Margin	6.2 db	14.4 db
Line Coding	1	1
Output Power	14.0 dBm	14.4 dBm
Actual Delay	3 ms	5 ms
Actual INP	2.0 symbols	7.0 symbols
Previous Data Rate	0 kbps	0 kbps
15M CV	0	0
15M FEC	0	0
15M FECS	0	0
15M Elapsed time	844 secs	757 secs
15M ES	0	0
15M SES	0	0
15M LOSS	0	0
15M UAS	0	0
1Day CV	0	0
1Day FEC	0	0
1Day FECS	0	0
1Day Elapsed time	86344 secs	86257 secs
1Day ES	0	0
1Day SES	0	0
1Day LOSS	0	0
1Day UAS	0	0
Refresh		

## ARP Table

This table stores mapping information that the device uses to find the Layer 2 Media Access Control (MAC) address that corresponds to the Layer 3 IP address of the device via the Address Resolution Protocol (ARP) feature.

Status

▼ ARP Table

Wired & Wireless

IP Address	MAC Address	Interface	Static ARP
192.168.1.100	00:05:5D:6A:58:D2	lan	No

**IP Address:** Shows the IP Address of the device that the MAC address maps to.

**MAC Address:** Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

**Interface:** Shows the interface name (on the router) that this IP address connects to.

**Static ARP:** Shows the status of static ARP.

## DHCP Table

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.

Status			
▼ DHCP Table			
Leased Table			
IP Address ▶	MAC Address	Client Host Name	Register Information

**IP Address:** The IP address which is assigned to the host with this MAC address.

**MAC Address:** The MAC Address of internal dhcp client host.

**Client Host Name:** The Host Name of internal dhcp client.

**Register Information:** Shows the information provided during registration.

# System Log

Display system logs accumulated up to the present time. You can trace its historical information with this function.

Status

System Log

Current Time: Sat Jan 1 00:27:28 2000

Jan 1 00:00:10 FDNSLOGIN: init  
Jan 1 00:00:10 FDNSLOGIN: begin service loop for FakedDnsProxy  
Jan 1 00:00:10 PPOELOGIN: proxy service :10080 ready  
Jan 1 00:00:18 dnsmasq[242]: using nameserver 210.241.192.201#53  
Jan 1 00:00:18 dnsmasq[242]: using nameserver 168.95.1.1#53  
Jan 1 00:00:19 UPNPD[260]: HTTP listening on port 2800  
Jan 1 00:00:19 UPNPD[260]: uuidvalue=uuid:28802880-2880-1880-a880-7000626f6f04  
Jan 1 00:00:28 DHCP SERVER: DHCPDISCOVER from 00:05:5d:6a:58:d2 via br0  
Jan 1 00:00:28 DHCP SERVER: DHCP offer to 00:05:5d:6a:58:d2  
Jan 1 00:00:28 DHCP SERVER: DHCP request from 00:05:5d:6a:58:d2  
Jan 1 00:00:28 DHCP SERVER: DHCP ack to 00:05:5d:6a:58:d2  
Jan 1 00:03:37 syslog: webs: admin (192.168.1.100) login...  
Jan 1 00:05:26 DHCP SERVER: DHCPINFORM from 192.168.1.100  
Jan 1 00:05:29 DHCP SERVER: DHCPINFORM from 192.168.1.100

RefreshClear

**Refresh:** Click to update the system log.

**Clear:** Click to clear the current log from the screen.

Status

System Log

Current Time: Sat Jan 1 00:27:48 2000

RefreshClear

## Firewall Log

Firewall Log displays the log information of any unexpected events that occurs to your firewall settings. This page displays the router Firewall Log entries which have been recorded when you have enabled Intrusion Detection or Block WAN PING in the Configuration – Firewall section of the interface. Please see the Firewall section of this manual for more details on how to enable Firewall event logging.

**Status**

**Firewall Log**

Current Time: Thu Jul 2 08:29:29 2009

Jul 2 08:28:44 URLFilter: [Domain] TCP packet from [br0] 192.168.1.101:29581 to 203.84.202.164:80

Refresh Clear

## UPnP Portmap


This section lists all the established port-mapping using UPnP (Universal Plug and Play).

Status

▼UPnP Portmap

Table

Name	Protocol	External Port	Internal Port	IP Address
------	----------	---------------	---------------	------------



**Name:** The Host Name of the internal UPNP client.

**Protocol:** The connection protocol of the UPNP client.

**External Port:** The external port for this connection.

**Internal Port:** The internal port for this connection.

**IP Address:** IP of the internal UPNP client.

# Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

[LAN](#), [WAN](#), [System](#), [Firewall](#), [QoS](#), [Virtual Server](#), [Wake on LAN](#), [Time Schedule](#) and [Advanced](#).

The function of each configuration sub-item is described in the following sections.

▼ Configuration
▶ LAN
▶ WAN
▶ System
▶ Firewall
▪ QoS
▶ Virtual Server
▪ Wake on LAN
▪ Time Schedule
▶ Advanced

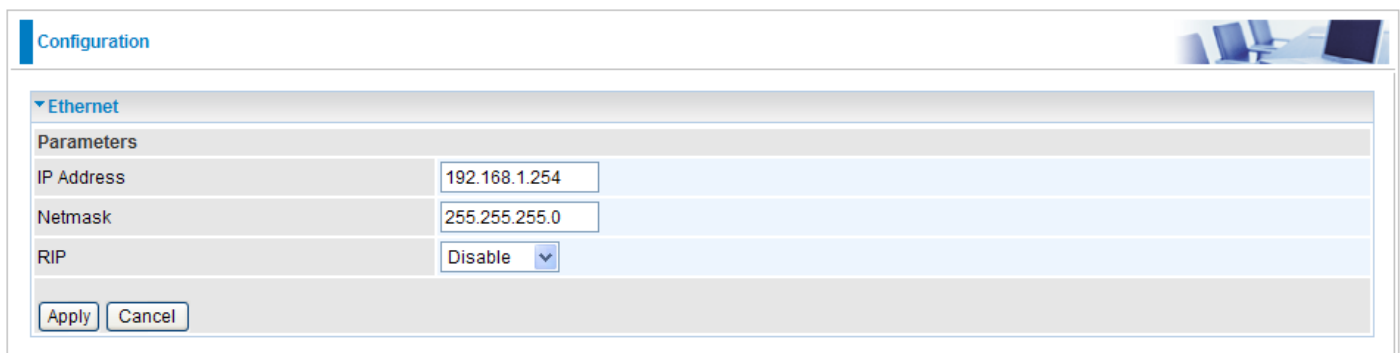
## LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building or just within the same storey of a building.

There are 6 items within the LAN section: [Ethernet](#), [IP Alias](#), [Wireless](#), [Wireless Security](#), [WPS](#) and [DHCP Server](#).

### Ethernet

The router supports more than one Ethernet IP addresses in the LAN that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



The screenshot shows the 'Configuration' page of a router. Under the 'Ethernet' section, there is a 'Parameters' table. The table has three rows: 'IP Address' with the value '192.168.1.254', 'Netmask' with the value '255.255.255.0', and 'RIP' with a dropdown menu set to 'Disable'. At the bottom of the table are 'Apply' and 'Cancel' buttons.

Parameters	
IP Address	192.168.1.254
Netmask	255.255.255.0
RIP	Disable

Apply Cancel

**IP Address:** The default IP on this router.

**Netmask:** The default subnet mask on this router.

**RIP:** RIP v1, RIP v2 Broadcast, RIP v2 Multicast and RIP v1+v2 Broadcast. Check to enable RIP function.

Click Apply to confirm the settings.



## IP Alias

This function allows the addition an IP alias to the network interface. It further allows user the flexibility to assign a specific function to use this IP.

Configuration

▼ IP Alias

Parameters

IP Address	Netmask
<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/>	<input type="button" value="Edit / Delete"/>

**IP Address:** Enter the IP address to be added to the network.

**Netmask:** Specify a subnet mask for the IP to be added.

Click Apply to confirm the settings.

## Wireless

Configuration

Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11g + n
Number of Active SSID	1
SSID No.	<input checked="" type="radio"/> SSID1
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx PowerLevel	100 (0 ~ 100)
AP MAC Address	00:04:ED:12:4B:F0
AP Firmware Version	Billion 1.1.1
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Wireless Distribution System (WDS)

WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	<div>1. <input type="text"/></div> <div>2. <input type="text"/></div> <div>3. <input type="text"/></div> <div>4. <input type="text"/></div>

\*\* WDS depends on the settings of main security encryption type. \*\*

Apply

Cancel

Security settings ▶

### Parameters

**WLAN Service:** Default setting is set to Enable. If you do not have any wireless, select Disable.

**Mode:** The default setting is 802.11g+n. If you do not know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b. And if you have 11n card, you can select 802.11n.

**Number of Active SSID:** You can select 1, 2, or 4 SSIDs to be available at the same time.

**SSID No.:** The selection of SSIDs will depend on the Number of Active SSID. Select each SSID, ranging from SSID1, SSID2, SSID3 and SSID4 and set their individual configurations.

Number of Active SSID	4
SSID No.	<input checked="" type="radio"/> SSID1 <input type="radio"/> SSID2 <input type="radio"/> SSID3 <input type="radio"/> SSID4

**ESSID:** The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

**Hide ESSID:** This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

**Enable:** When enabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.

**Disable:** When disabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

**Regulation Domain:** There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

**Channel ID:** Select the wireless connection channel ID that you would like to use.

**Note:** *Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).*

**Channel Width:** Select either 20 MHz or 20/40 MHz for the channel bandwidth. The higher the bandwidth the better the performance will be.

**TX PowerLevel:** It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

**Note:** *The Power Level maybe different in each access network user premise environment, choose the most suitable level for your network.*

**AP MAC Address:** It is a unique hardware address of the Access Point.

**AP Firmware Version:** The Access Point firmware version.

**WPS Service:** Select Enable if you would like to activate WPS service.

**WPS State:** This column allows you to set the status of the device wireless setting whether it has been configured or unconfigured. For WPS configuration please refer to the section on [Wi-Fi Network Setup](#) for detail.

**WMM:** This feature is used to control the prioritization of traffic according to 4 Access categories: Voice, Video, Best Effort and Background. Default is set to disable.

### **Wireless Distribution System (WDS)**

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantages of the cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

**WDS Service:** The default setting is disabled. Check **Enable** radio button to activate this function.

1. **Peer WDS MAC Address:** It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
2. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.
3. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

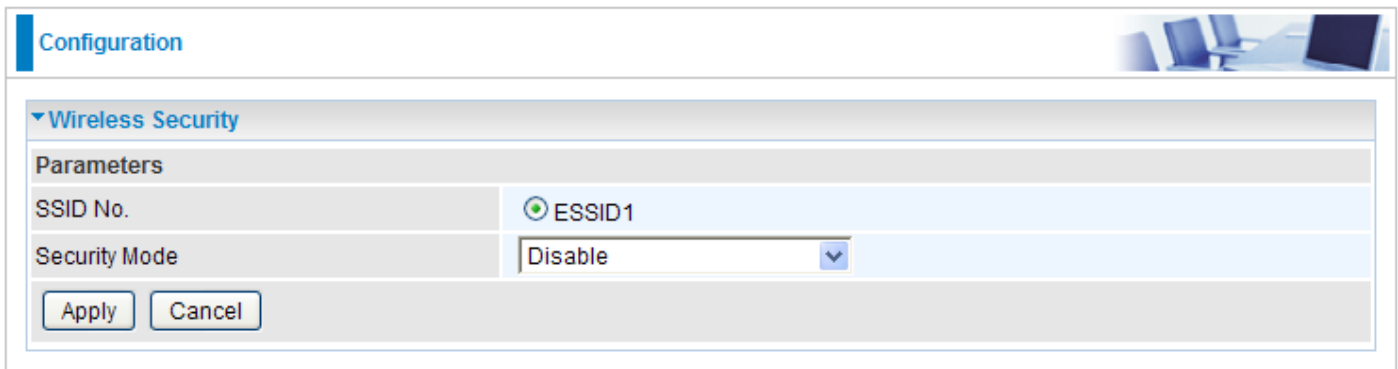
**Note:** *For MAC Address, the format can be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.*

Click Apply to confirm the settings.

You can click Security settings link next to Cancel button to go to Wireless Security screen (see **Wireless Security** section).

## Wireless Security

You can disable or enable wireless security function using WPA or WEP for protecting wireless network. The default mode of wireless security is disabled.

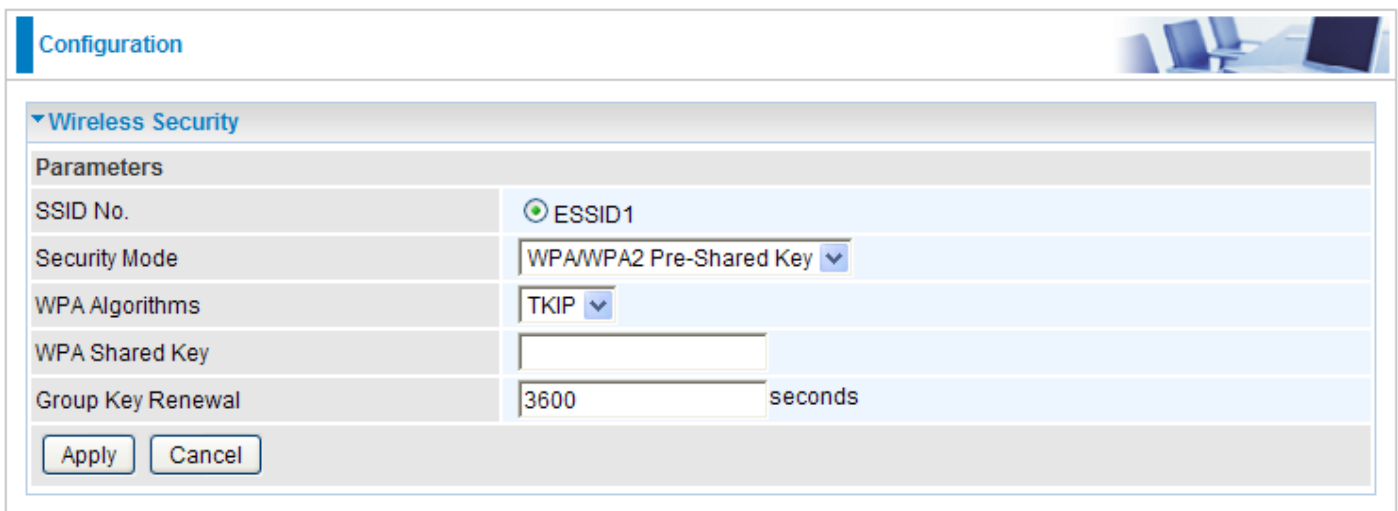


The screenshot shows a 'Configuration' window with a 'Wireless Security' section. Under 'Parameters', the 'SSID No.' is set to 'ESSID1' and the 'Security Mode' is set to 'Disable'. There are 'Apply' and 'Cancel' buttons at the bottom.

**SSID No.:** The selection of SSIDs will depend on the Number of Active SSID set on Wireless screen.

**Security Mode:** Select the security mode from the drop-down menu, there are Disable, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key and WEP.

### WPA / WPA2 / WPA/WPA2 Pre-Shared Key



The screenshot shows the 'Wireless Security' configuration window with 'Security Mode' set to 'WPA/WPA2 Pre-Shared Key'. Other settings include 'WPA Algorithms' set to 'TKIP', 'WPA Shared Key' as an empty text field, and 'Group Key Renewal' set to '3600 seconds'. 'Apply' and 'Cancel' buttons are at the bottom.


**Security Mode:** You can choose the type of security mode you want to apply from the drop-down menu.

**WPA Algorithms:** There are 3 types of the WPA-PSK, WPA2-PSK and WPA/WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

**WPA Shared Key:** The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

**Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

Click Apply to confirm the settings.

Configuration


Wireless Security

Parameters

SSID No.	<input checked="" type="radio"/> ESSID1	
Security Mode	WEP	
WEP Authentication	Open System	
Default Used WEP Key	<input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Passphrase (Generate Key)	<input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/>	
Key 1	Hex	<input type="text"/>
Key 2	Hex	<input type="text"/>
Key 3	Hex	<input type="text"/>
Key 4	Hex	<input type="text"/>

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33.  
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.  
WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.  
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

**Security Mode:** Choose the type of security mode **WEP** from the drop-down menu.

**WEP Authentication:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. There are 3 options to select from: **Open System**, **Shared Key** or **Both**.

**Default Used WEP Key:** Select the encryption key ID; please refer to **Key (1~4)** below.

**Passphrase:** This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

**Key (1~4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 or 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Click Apply to confirm the settings.

## WPS

WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi networks for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method & PBC Method.**

Configuration

▼ WPS

Parameters

WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Role	<input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee
WPS PIN	42776260
Enrollee's PIN	<input type="text"/>

Start

Cancel

## Wi-Fi Network Setup

### PIN Method: Configure AP as Registrar

1. Jot down the client's Pin (eg. 16837546).

**Configuration**

▼ WPS

Parameters

WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Role	<input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee
WPS PIN	25879810
Enrollee's PIN	<input type="text" value="16837546"/>

2. Enter the Enrollee's PIN number and then press Start.
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

←

Profile

Network

Advanced

Statistics

WMM

**WPS**

Radio On/Off

About

→

WPS AP List

ID : 0x0000	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-00-00-01	1

WPS Profile List

PIN

PBC

☒ WPS Associate IE  
☒ WPS Probe IE

Progress >> 0%  
WPS status is disconnected

Rescan

Information

Pin Code

Config Mode  
Enrollee

Detail

Connect

Rotate

Disconnect

Export Profile

Delete

Status >> Disconnected  
Extra Info >>  
Channel >>  
Authentication >>  
Encryption >>  
Network Type >>  
IP Address >>  
Sub Mask >>  
Default Gateway >>

HT  
BW >> n/a  
GI >> n/a  
MCS >> n/a  
SNR0 >> n/a  
SNR1 >> n/a

Link Quality >> 0%  
Signal Strength 1 >> 0%  
Signal Strength 2 >> 0%  
Noise Strength >> 0%

Transmit  
Link Speed >> Max  
Throughput >> 0.000 Kbps

Receive  
Link Speed >> Max  
Throughput >> 0.000 Kbps



4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.

The screenshot displays a network management interface with a top navigation bar containing icons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** A table showing two entries for 'wlan-ap' with MAC addresses 00-1D-92-C0-13-CD and 00-04-ED-38-F7-2E, both with a count of 1.
- WPS Profile List:** A section for the 'wlan-ap' profile showing a progress bar at 100% and a status message: 'PIN - Get WPS profile successfully.'
- WPS Configuration:** A section with checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. Below them are buttons for 'PIN' and 'PBC'.
- WPS Status and Performance:** A section on the right showing various status indicators and performance metrics.
  - Link Quality >> 100%** (Green bar)
  - Signal Strength 1 >> 64%** (Yellow bar)
  - Signal Strength 2 >> 34%** (Red bar)
  - Noise Strength >> 26%** (Green bar)
  - Transmit:** Link Speed >> 270.0 Mbps, Throughput >> 5.600 Kbps. A graph shows a peak of 38.624 Kbps.
  - Receive:** Link Speed >> 54.0 Mbps, Throughput >> 81.608 Kbps. A graph shows a peak of 146.840 Kbps.
- General Information:** A section on the left providing details about the 'wlan-ap' profile, including its status, extra info, channel, authentication, encryption, network type, IP address, sub mask, and default gateway.

**General Information:**

- Status >> wlan-ap <-> 00-1D-92-C0-13-CD
- Extra Info >> Link is Up [TxPower:100%]
- Channel >> 1 <-> 2412 MHz; central channel : 3
- Authentication >> Open
- Encryption >> NONE
- Network Type >> Infrastructure
- IP Address >> 192.168.1.100
- Sub Mask >> 255.255.255.0
- Default Gateway >> 192.168.1.254

**HT (High Throughput) Settings:**

- BW >> 40
- GI >> long
- MCS >> 15
- SNR0 >> 19
- SNR1 >> n/a

## PIN Method: Configure AP as Enrollee

1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (eg. 25879810).

**Configuration**

**WPS**

**Parameters**

WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Role	<input type="radio"/> Registrar <input checked="" type="radio"/> Enrollee
WPS PIN	25879810
Mode	PIN

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

Profile Network Advanced Statistics WMM WPS Radio On/Off About

**WPS AP List**

ID : 0x0000	wlan-ap	00-1D-92-C0-13-CD	1
ID :	D2-VPN	00-1B-11-E4-DA-D5	7

**WPS Profile List**

ExRegNWEA4036

☒ WPS Associate IE

☒ WPS Probe IE

**Status >> Disconnected**

**Extra Info >>**

**Channel >>**

**Authentication >>**

**Encryption >>**

**Network Type >>**

**IP Address >>**

**Sub Mask >>**

**Default Gateway >>**

**HT**

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

**Link Quality >> 0%**

**Signal Strength 1 >> 0%**

**Signal Strength 2 >> 0%**

**Noise Strength >> 0%**

**Transmit**

**Link Speed >>** Max

**Throughput >>** 0.000 Kbps

**Receive**

**Link Speed >>** Max

**Throughput >>** 0.000 Kbps

- The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.

**WPS AP List**

ID	MAC	Priority
ExRegNWEA4036	00-1D-92-C0-13-CD	1
wlan-ap	00-04-ED-38-F7-2E	1

**WPS Profile List**

ExRegNWEA4036

**WPS Associate IE** ☒ **WPS Probe IE** ☒

Progress >> 100%

PIN - Get WPS profile successfully.

**Rescan**  
**Information**  
**Pin Code**  
25879810 **Renew**  
**Config Mode**  
Registrar  
**Detail**  
**Connect**  
**Rotate**  
**Disconnect**  
**Export Profile**

**Status >>** ExRegNWEA4036 <-> 00-1D-92-C0-13-CD  
**Extra Info >>** Link is Up [TxPower:100%]  
**Channel >>** 1 <-> 2412 MHz; central channel : 3  
**Authentication >>** WPA2-PSK  
**Encryption >>** AES  
**Network Type >>** Infrastructure  
**IP Address >>** 192.168.1.100  
**Sub Mask >>** 255.255.255.0  
**Default Gateway >>** 192.168.1.254

**HT**

BW >> 40 SNR0 >> 20  
GI >> long MCS >> 14 SNR1 >> n/a

**Link Quality >> 100%**  
**Signal Strength 1 >> 65%**  
**Signal Strength 2 >> 39%**  
**Noise Strength >> 26%**

**Transmit**  
**Link Speed >>** 243.0 Mbps  
**Throughput >>** 0.000 Kbps

**Receive**  
**Link Speed >>** 40.5 Mbps  
**Throughput >>** 98.612 Kbps

- Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.

Profile
 Network
 Advanced
 Statistics
 WMM
 WPS
 Radio On/Off
 About

WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-22-22-23	1

WPS Profile List

ExRegNWEA4036

PIN

PBC

☒ WPS Associate IE
 ☒ WPS Probe IE

Progress >> 0%

WPS status is disconnected

Rescan

Information

Pin Code

25879810 Renew

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

SSID >>

ExRegNWEA4036

BSSID >>

00-00-00-00-00-00

Authentication Type >>

WPA2-PSK

Encryption Type >>

AES

Key Length >>

5

Key Index >>

1

Key Material >>

811B5B9F3403DCB08BA73BF3E4787581C37DC4BDD147C4E62526D4E8C39DBF78

☒ Show Password

OK

Cancel

Wireless

Parameters

WLAN Service

☒ Enable
 ☐ Disable

Mode

802.11g + n

Number of Active SSID

1

SSID No.

☒ SSID1

ESSID

ExRegNWEA4036

Hide ESSID

☐ Enable
 ☒ Disable

Regulation Domain

N.America

Channel ID

Channel 1 (2.412 GHz)

Channel Width

20/40MHZ

Tx Power Level

100 (0 ~ 100)

AP MAC Address

00:1D:92:C0:13:CD

AP Firmware Version

1.1.7.0

WPS Service

☒ Enable
 ☐ Disable

WPS State

☒ Configured
 ☐ Unconfigured

WMM

☐ Enable
 ☒ Disable

Wireless Distribution System (WDS)

WDS Service

☐ Enable
 ☒ Disable

Peer WDS MAC address

1.

2.

3.

4.

Apply

Cancel

Security settings

▼Wireless Security

Parameters

SSID No.

ESSID1

Security Mode

WPA2 Pre-Shared Key

WPA Algorithms

AES

WPA Shared Key

811B5B9F3403DCB08I

Group Key Renewal

3600

seconds

Apply

Cancel

## PBC Method:

1. Press the PBC button of the AP.
2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.

The screenshot displays the Ralink WPS Utility interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. Below the navigation bar, the main area is divided into several sections:

- WPS AP List:** A table showing two available APs:

ID	SSID	BSSID	Signal
00-04-ED-00-00-01	wlan-ap	00-04-ED-00-00-01	1
00-1D-92-C0-13-CD	wlan-ap	00-1D-92-C0-13-CD	1
- WPS Profile List:** A section for managing WPS profiles, currently empty.
- WPS Status:** Shows the current WPS status as "Disconnected". It includes checkboxes for "WPS Associate IE" and "WPS Probe IE", both of which are checked. A progress bar indicates "Progress >> 0%".
- WPS Configuration:** A section on the right side of the interface containing buttons for "Rescan", "Information", "Pin Code" (with a field showing "16837546" and a "Renew" button), "Config Mode" (set to "Enrollee"), "Detail", "Connect", "Rotate", "Disconnect", "Export Profile", and "Delete".
- Link Quality:** A section showing various link quality metrics:

Metric	Value
Link Quality	>> 0%
Signal Strength 1	>> 0%
Signal Strength 2	>> 0%
Noise Strength	>> 0%
- Transmit/Receive Performance:** Two sections showing performance metrics and graphs:

Metric	Value
Transmit Link Speed	>> 8.800 Kbps
Throughput	>> 8.800 Kbps
Receive Link Speed	>> 147.408 Kbps
Throughput	>> 147.408 Kbps

- When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

The screenshot displays the WPS (Wi-Fi Protected Setup) configuration interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. Below the navigation bar, the interface is divided into several sections:

- WPS AP List:** A table showing two available access points.
 

ID	SSID	BSSID	Signal
wlan-ap	wlan-ap	00-1D-92-C0-13-CD	1
wlan-ap	wlan-ap	00-04-ED-38-F7-2E	1
- WPS Profile List:** A section showing the selected profile 'wlan-ap' and its configuration options.
 

Option	Status
PIN	<input checked="" type="checkbox"/> WPS Associate IE
PBC	<input checked="" type="checkbox"/> WPS Probe IE

Progress >> 100%

PBC - Get WPS profile successfully.
- Right Panel:** A vertical sidebar containing buttons for Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, and Delete.
- Status Section:**
  - Status >> wlan-ap <--> 00-1D-92-C0-13-CD
  - Extra Info >> Link is Up [TxPower:100%]
  - Channel >> 1 <--> 2412 MHz; central channel : 3
  - Authentication >> Open
  - Encryption >> NONE
  - Network Type >> Infrastructure
  - IP Address >> 192.168.1.100
  - Sub Mask >> 255.255.255.0
  - Default Gateway >> 192.168.1.254
- HT Section:**
  - BW >> 40
  - GI >> long
  - MCS >> 14
  - SNR0 >> 20
  - SNR1 >> n/a
- Link Quality Section:**
  - Link Quality >> 100%
  - Signal Strength 1 >> 60%
  - Signal Strength 2 >> 44%
  - Noise Strength >> 26%
- Transmit Section:**
  - Link Speed >> 243.0 Mbps
  - Throughput >> 0.192 Kbps
- Receive Section:**
  - Link Speed >> 81.0 Mbps
  - Throughput >> 93.732 Kbps

## Wi-Fi Network Setup with Windows Vista WCN:

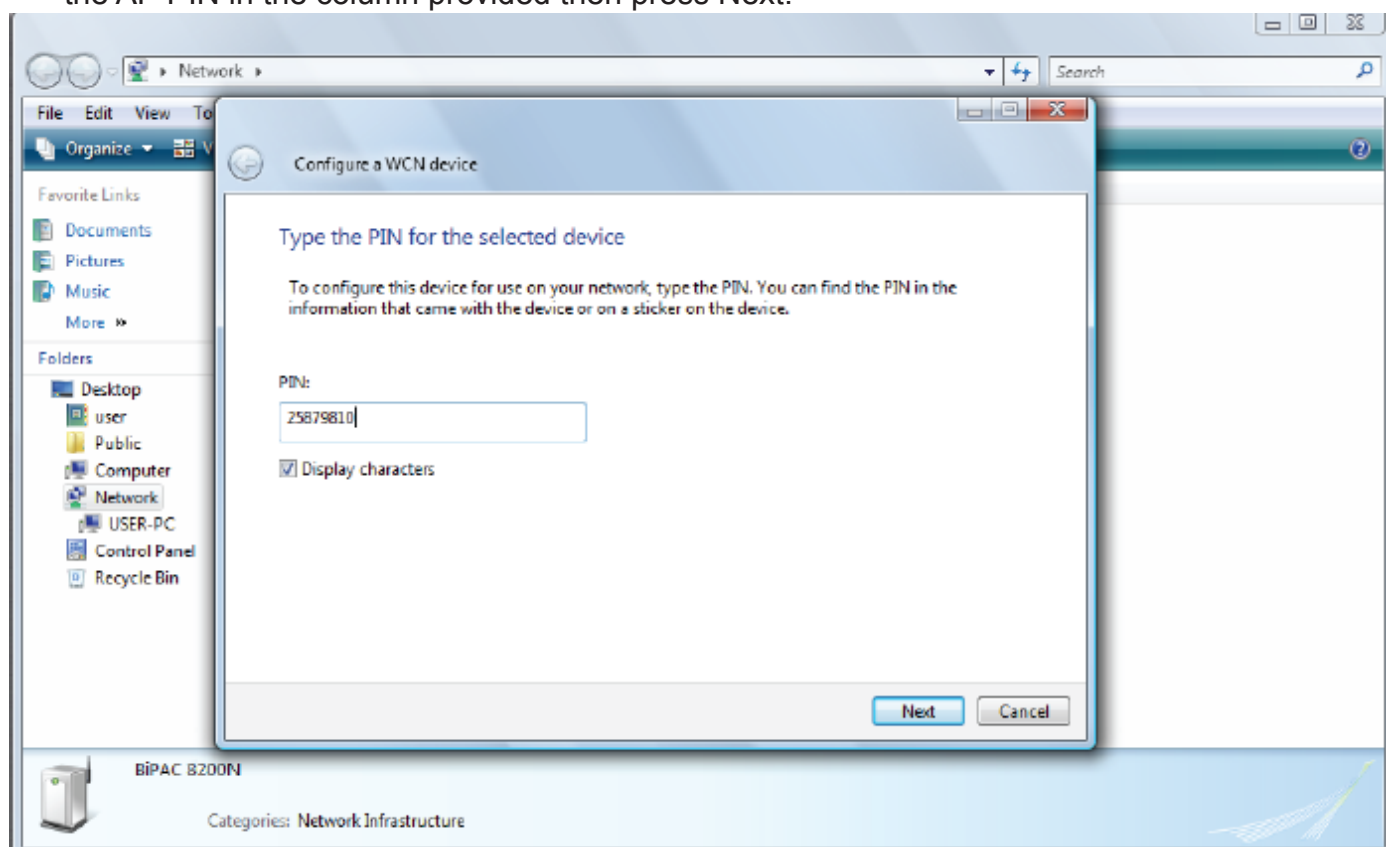
1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Enable WPS service, set the WPS State to Unconfigured and then click Apply.

The screenshot shows a web-based configuration interface for a wireless network. The 'Wireless' section is expanded, showing various parameters. The 'WLAN Service' is set to 'Enable'. The 'Mode' is set to '802.11g + n'. The 'Number of Active SSID' is set to '1'. The 'SSID No.' is set to 'SSID1'. The 'ESSID' is set to 'wlan-ap'. The 'Hide ESSID' is set to 'Disable'. The 'Regulation Domain' is set to 'N.America'. The 'Channel ID' is set to 'Channel 1 (2.412 GHz)'. The 'Channel Width' is set to '20/40MHZ'. The 'Tx Power Level' is set to '100'. The 'AP MAC Address' is '00:1D:92:C0:13:CD'. The 'AP Firmware Version' is '1.1.7.0'. The 'WPS Service' is set to 'Enable'. The 'WPS State' is set to 'Unconfigured'. The 'WMM' is set to 'Disable'. The 'Wireless Distribution System (WDS)' section shows 'WDS Service' set to 'Disable'. The 'Peer WDS MAC address' section has four empty input fields. At the bottom, there are 'Apply', 'Cancel', and 'Security settings' buttons.

Parameters	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11g + n
Number of Active SSID	1
SSID No.	<input checked="" type="radio"/> SSID1
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	1.1.7.0
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

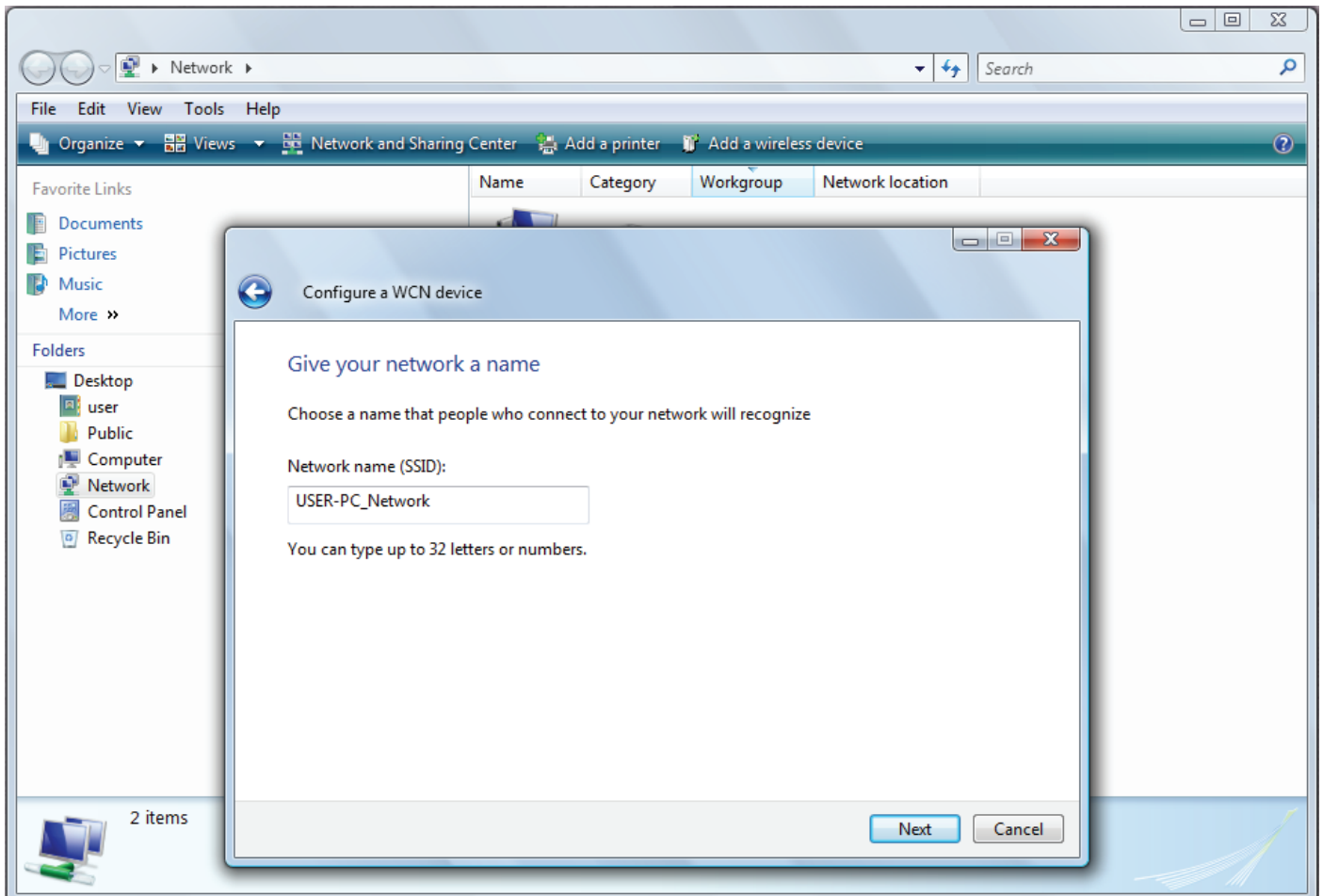
Apply Cancel Security settings

3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 8200N icon and enter the AP PIN in the column provided then press Next.

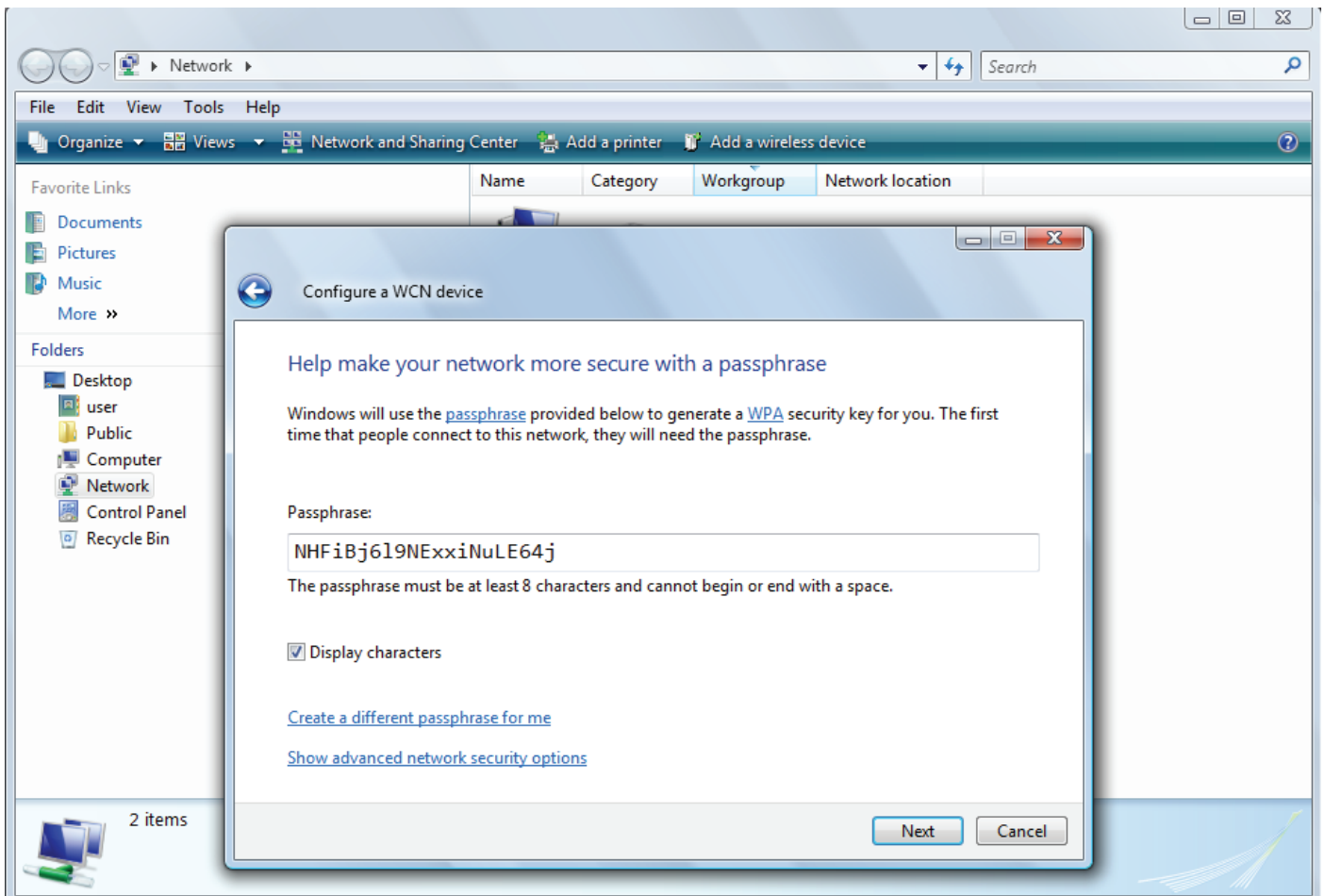




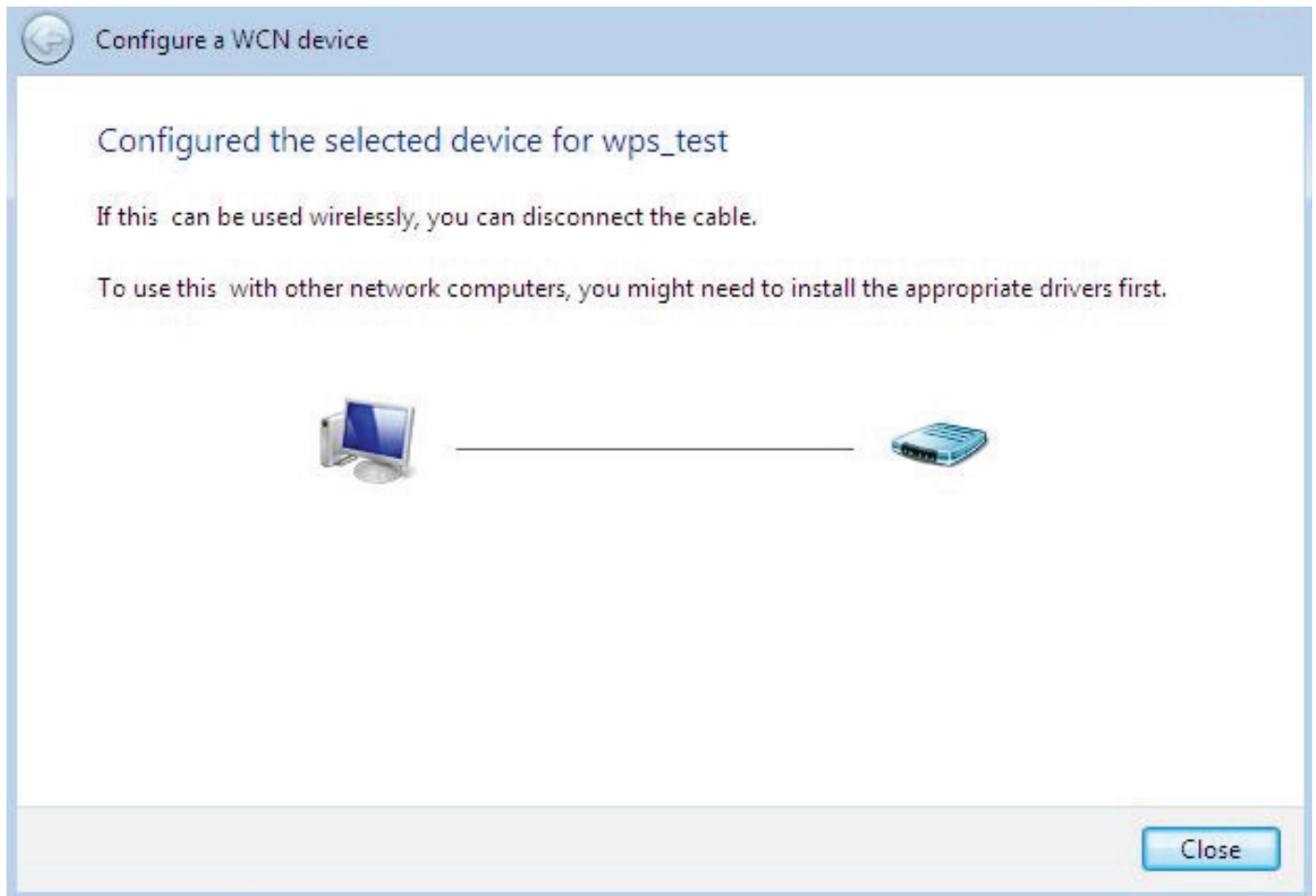
4. Enter the AP SSID then click Next.



5. Enter the passphrase then click Next.



6. When you have come to this step, you will have completed the Wi-Fi network setup using the built-in WCN feature in Windows Vista.



## DHCP Server

DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device.

Configuration

▼ DHCP Server

Parameters

DHCP Server Mode	DHCP Server ▼	
Domain Name	home.gateway	
Range Start	192.168.1.100	
Range End	192.168.1.199	
Default Lease Time	43200	seconds
Maximum Lease Time	86400	seconds
Use Router as DNS Server	<input checked="" type="checkbox"/>	
Primary DNS Server Address		
Secondary DNS Server Address		

Apply

 Fixed Host ▶

Current Mode: DHCP Server

To configure the router's DHCP Server, select **DHCP Server** from the DHCP Server Mode drop-down menu. You can then configure parameters of the DHCP Server including the domain, IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. If you check "Use Router as a DNS Server", the Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network). Click Apply to enable this function.

If you select **DHCP Relay** from the DHCP Server Mode drop-down menu, you must enter the IP address of the DHCP server that assigns an IP address to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click Apply to enable this function.

Configuration

▼ DHCP Server

Parameters

DHCP Server Mode	DHCP Relay ▼	
DHCP Relay Server		

Apply

Current Mode: DHCP Server

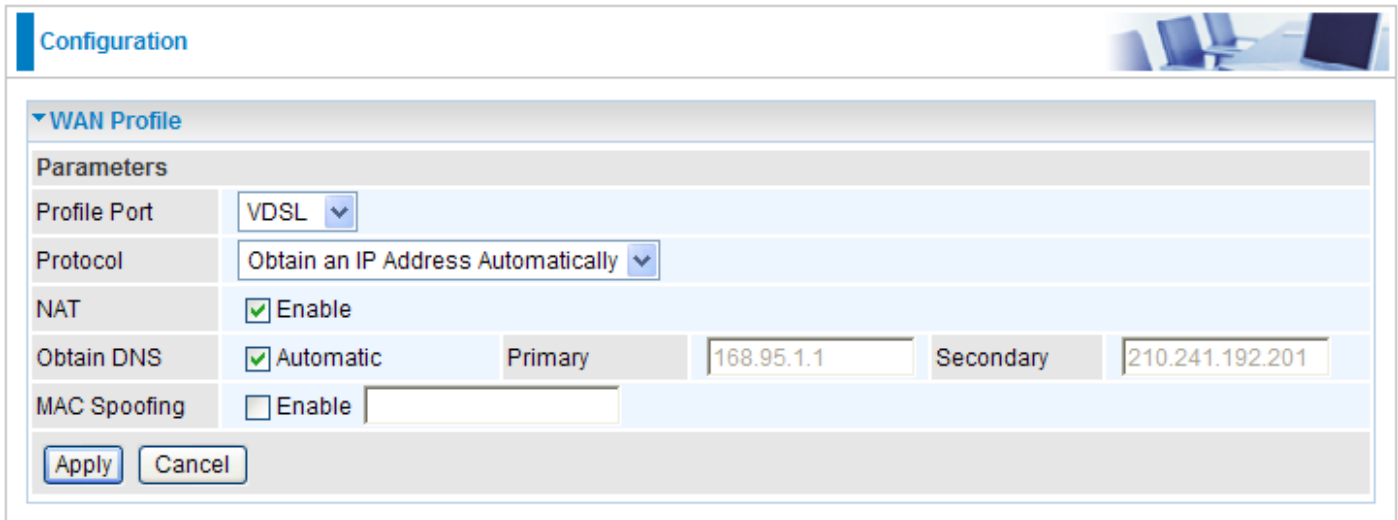
## WAN - Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems.

### WAN Profile - Main Port: VDSL

#### Obtain an IP Address Automatically (VDSL)

When connecting to the ISP, your router also functions as a DHCP client. By configuring DHCP settings, the device is able to obtain IP settings automatically from the ISP.



The screenshot shows a web-based configuration interface for a WAN profile. The title bar says "Configuration" and includes a small image of a laptop and chairs. Below the title bar, there is a section titled "WAN Profile" with a dropdown arrow. Under this section, there is a "Parameters" table. The table has the following rows: "Profile Port" with a dropdown menu showing "VDSL"; "Protocol" with a dropdown menu showing "Obtain an IP Address Automatically"; "NAT" with a checked checkbox and the text "Enable"; "Obtain DNS" with a checked checkbox and the text "Automatic", followed by two input fields labeled "Primary" and "Secondary" containing the IP addresses "168.95.1.1" and "210.241.192.201" respectively; and "MAC Spoofing" with an unchecked checkbox and the text "Enable", followed by an empty input field. At the bottom of the parameters section, there are two buttons: "Apply" and "Cancel".

Parameters					
Profile Port	VDSL				
Protocol	Obtain an IP Address Automatically				
NAT	<input checked="" type="checkbox"/> Enable				
Obtain DNS	<input checked="" type="checkbox"/> Automatic	Primary	168.95.1.1	Secondary	210.241.192.201
MAC Spoofing	<input type="checkbox"/> Enable				

Apply Cancel

**Protocol:** Select the protocol you will use in the device.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**Obtain DNS:** Select this check box to activate DNS.

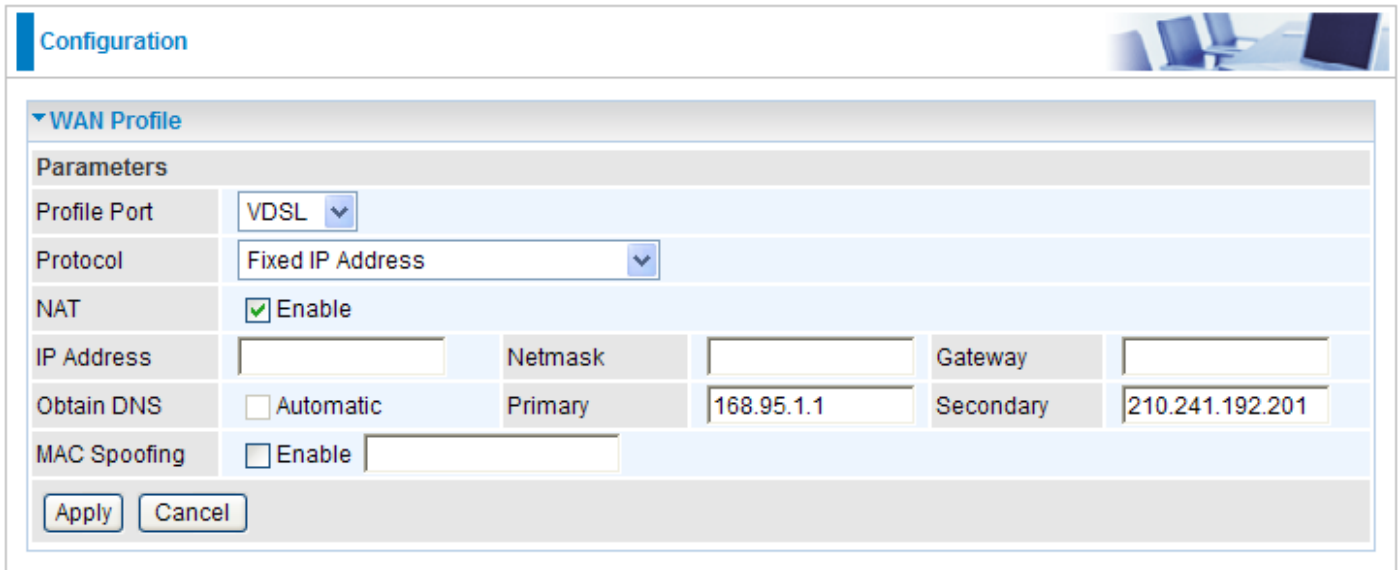
**Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

**MAC Spoofing:** This option is required by some service providers. You must fill the MAC address specified by your service provider when this information is required. It will temporarily change your router's MAC address to the one you have specified in this field. The default setting is set to disable.

Click Apply to confirm the settings.

## Fixed IP Address (VDSL)

A Static WAN connection will be configured according to the IP properties defined by your ISP.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a 'WAN Profile' section is expanded, showing a 'Parameters' table. The table has the following rows: 'Profile Port' with a dropdown set to 'VDSL'; 'Protocol' with a dropdown set to 'Fixed IP Address'; 'NAT' with a checked 'Enable' checkbox; 'IP Address' with an empty text field; 'Netmask' with an empty text field; 'Gateway' with an empty text field; 'Obtain DNS' with an unchecked 'Automatic' checkbox; 'Primary' with the text '168.95.1.1'; 'Secondary' with the text '210.241.192.201'; and 'MAC Spoofing' with an unchecked 'Enable' checkbox and an empty text field. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Parameters					
Profile Port	VDSL				
Protocol	Fixed IP Address				
NAT	<input checked="" type="checkbox"/> Enable				
IP Address		Netmask		Gateway	
Obtain DNS	<input type="checkbox"/> Automatic	Primary	168.95.1.1	Secondary	210.241.192.201
MAC Spoofing	<input type="checkbox"/> Enable				

Apply Cancel

**Protocol:** Select the protocol you will use in the device.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**IP Address:** Enter your fixed IP address. Each IP address entered in the field must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

**Netmask:** User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

**Gateway:** Enter the IP address of the default gateway (if given).

**Obtain DNS:** Select this check box to activate DNS.

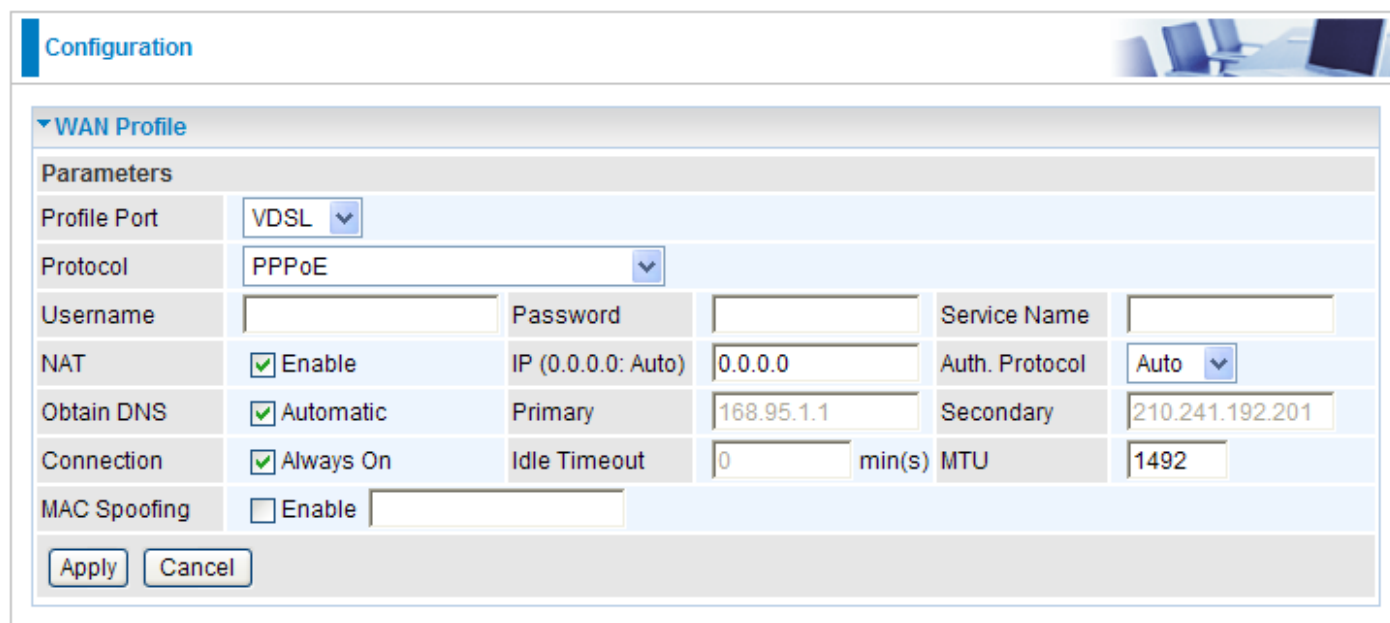
**Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

**MAC Spoofing:** This option is required by some service providers. You must fill the MAC address specified by your service provider when this information is required. It will temporarily change your router's MAC address to the one you have specified in this field. The default setting is set to disable.

Click Apply to confirm the settings.

## PPPoE (VDSL)

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



The screenshot shows a web-based configuration interface for a WAN Profile. The 'WAN Profile' section is expanded, showing a 'Parameters' table. The 'Profile Port' is set to 'VDSL' and the 'Protocol' is set to 'PPPoE'. The 'Username' and 'Password' fields are empty. The 'Service Name' field is empty. The 'NAT' checkbox is checked and labeled 'Enable'. The 'IP (0.0.0.0: Auto)' field is set to '0.0.0.0'. The 'Auth. Protocol' is set to 'Auto'. The 'Obtain DNS' checkbox is checked and labeled 'Automatic'. The 'Primary' DNS field is set to '168.95.1.1' and the 'Secondary' DNS field is set to '210.241.192.201'. The 'Connection' checkbox is checked and labeled 'Always On'. The 'Idle Timeout' field is set to '0' min(s). The 'MTU' field is set to '1492'. The 'MAC Spoofing' checkbox is unchecked and labeled 'Enable'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

WAN Profile					
Parameters					
Profile Port	VDSL				
Protocol	PPPoE				
Username		Password		Service Name	
NAT	<input checked="" type="checkbox"/> Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Auto
Obtain DNS	<input checked="" type="checkbox"/> Automatic	Primary	168.95.1.1	Secondary	210.241.192.201
Connection	<input checked="" type="checkbox"/> Always On	Idle Timeout	0 min(s)	MTU	1492
MAC Spoofing	<input type="checkbox"/> Enable				

Apply Cancel

**Protocol:** Select the protocol you will use in the device.

**Username:** Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

**Password:** Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

**Service Name:** This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**IP (0.0.0.0.Auto):** Enter your fixed IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

**Auth. Protocol:** Default is Auto. Please consult your ISP on whether to use Pap or Chap.

**Obtain DNS:** Select this check box to activate DNS.

**Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

**Connection:** Click on **Always On** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

**Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

**MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**MAC Spoofing:** This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. It will temporarily change your router's MAC address to the one you have specified in this field. The default setting is set to disable.

Click Apply to confirm the settings.

## Pure Bridge (VDSL)

Configuration

▼ WAN Profile

Parameters

Profile Port

VDSL ▼

Protocol

Pure Bridge ▼

Apply

Cancel

**Protocol:** Select the protocol you will use in the device.

Click Apply to confirm the change.

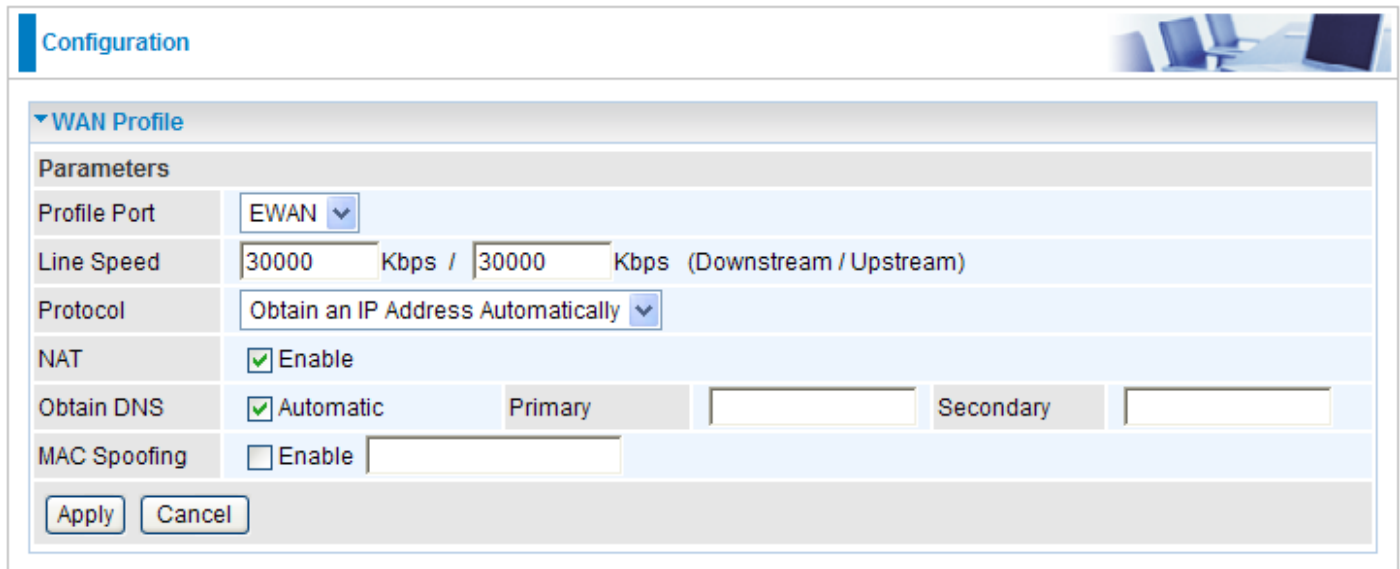


## WAN Profile - Main Port: EWAN

Besides using VDSL to get connected to the Internet, the VDSL router offers its Ethernet port 4 as a WAN port to be used to connect to Cable Modems and fibre optic lines. This alternative, yet faster method to connect to the internet will provide users with more flexibility to get online.

### Obtain an IP Address Automatically (EWAN)

When connecting to the ISP, your router also functions as a DHCP client. By configuring DHCP settings, the device is able to obtain IP settings automatically from the ISP.



**Configuration**

**WAN Profile**

**Parameters**

Profile Port: EWAN

Line Speed: 30000 Kbps / 30000 Kbps (Downstream / Upstream)

Protocol: Obtain an IP Address Automatically

NAT: ☒ Enable

Obtain DNS: ☒ Automatic Primary Secondary

MAC Spoofing: ☐ Enable

Apply Cancel

**Protocol:** Select the protocol you will use in the device.

**Line Speed:** Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

**Protocol:** Select the protocol you will use in the device.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**Obtain DNS:** Select this check box to activate DNS.

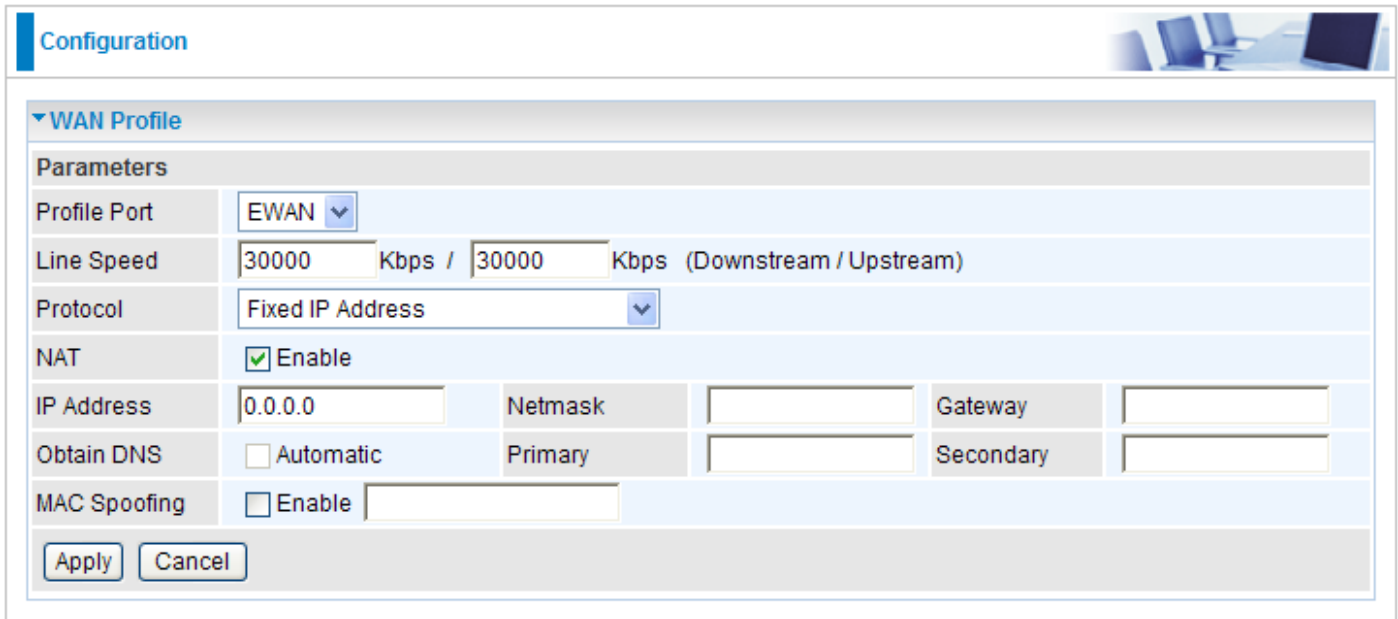
**Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

**MAC Spoofing:** This option is required by some service providers. You must fill the MAC address specified by your service provider when this information is required. It will temporarily change your router's MAC address to the one you have specified in this field. The default setting is set to disable.

Click Apply to confirm the settings.

## Fixed IP Address (EWAN)

A Static WAN connection will be configured according to the IP properties defined by your ISP.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, the 'WAN Profile' section is expanded. Under 'Parameters', the following settings are visible: 'Profile Port' is set to 'EWAN'; 'Line Speed' is set to '30000 Kbps / 30000 Kbps (Downstream / Upstream)'; 'Protocol' is set to 'Fixed IP Address'; 'NAT' is checked and labeled 'Enable'; 'IP Address' is set to '0.0.0.0'; 'Obtain DNS' is set to 'Automatic'; and 'MAC Spoofing' is unchecked. There are also input fields for 'Netmask', 'Gateway', 'Primary' DNS, and 'Secondary' DNS. At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

**Line Speed:** Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

**Protocol:** Select the protocol you will use in the device.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**IP Address:** Enter your fixed IP address. Each IP address entered in the field must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

**Netmask:** User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

**Gateway:** Enter the IP address of the default gateway (if given).

**Obtain DNS:** Select this check box to activate DNS.

**Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

**MAC Spoofing:** This option is required by some service providers. You must fill the MAC address specified by your service provider when this information is required. It will temporarily change your router's MAC address to the one you have specified in this field. The default setting is set to disable.

Click Apply to confirm the settings.

## PPPoE (EWAN)

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.

The screenshot shows a 'Configuration' window with a 'WAN Profile' section. Under 'Parameters', the following settings are visible:

- Profile Port:** EWAN (dropdown)
- Line Speed:** 30000 Kbps / 30000 Kbps (Downstream / Upstream)
- Protocol:** PPPoE (dropdown)
- Username:** [empty text box]
- Password:** [empty text box]
- Service Name:** [empty text box]
- NAT:** ☒ Enable
- IP (0.0.0.0: Auto):** 0.0.0.0
- Auth. Protocol:** Auto (dropdown)
- Obtain DNS:** ☒ Automatic
- Primary:** [empty text box]
- Secondary:** [empty text box]
- Connection:** ☒ Always On
- Idle Timeout:** 0 min(s)
- MTU:** 1492
- MAC Spoofing:** ☐ Enable [empty text box]

At the bottom are 'Apply' and 'Cancel' buttons.

**Line Speed:** Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

**Protocol:** Select the protocol you will use in the device.

**Username:** Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

**Password:** Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

**Service Name:** This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

**IP (0.0.0.0.Auto):** Enter your fixed IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

**Auth. Protocol:** Default is Auto. Please consult your ISP on whether to use Pap or Chap.

**Obtain DNS:** Select this check box to activate DNS.

**Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

**Connection:** Click on **Always On** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

**Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

**MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**MAC Spoofing:** This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. It will temporarily change your router's MAC address to the one you have specified in this field. The default setting is set to disable.

Click Apply to confirm the settings.

# System

There are the items within the System section: [Time Zone](#), [Firmware Upgrade](#), [Backup/Restore](#), [Restart](#), [User Management](#) and [Mail alert](#).


## Time Zone

Configuration

Time Zone

Parameters

Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Local Time Zone (+-GMT Time)	(GMT) Greenwich Mean Time	
SNTP Server IP Address	192.43.244.18	128.138.140.44
	129.6.15.29	131.107.1.10
Daylight Saving	<input checked="" type="checkbox"/> Automatic	
Resync Period	1440	minutes



Apply

Cancel

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the most current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

Click Apply to confirm the settings.

## Firmware Upgrade

Your router's firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.

Configuration

Firmware Upgrade

You may upgrade the system software on your network device.  
After upgrading, let your device restart with factory default settings or current settings.

Restart device with

☒ Factory Default Settings  
☐ Current Settings

New Firmware Image

**Factory Default Settings:** If select this setting, the device will reboot to restore the parameters of all its applications to its default values.

**Current Settings:** If select this setting, the device will reboot and retain the customized settings of all applications.

Click on Browse to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware to your router.

Firmware Upgrade

firmware upgrade progress

do not switch off device during flash update

total :

58%



**Warning**

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

## Backup / Restore

These functions allow you to save a backup of the current configuration of your router to a defined location on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup in hand in case any mistakes occur. It is advisable that you backup your router configuration before making any changes to your router configuration.

Configuration

▼ Backup/Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Backup

Restore Configuration

Configuration File

Browse...

Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

Restore

### Backup Configuration

Press Backup to select where on your local PC you want to store your setting file. You may also want to change the name of the file when saving if you wish to keep multiple backups.

### Restore Configuration

Press Browse to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router firmware. Settings files saved to your PC should not be manually edited in any way.

Select the settings files you wish to use, and press Restore to load the setting into the router. Click Restore to begin restoring the configuration and wait for the router to restart before performing any actions.

Restore Configuration

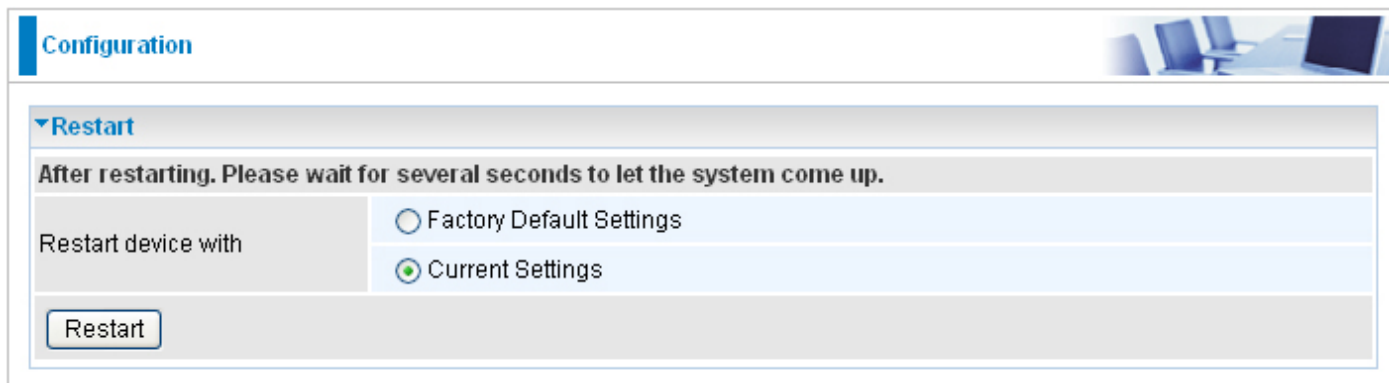
▼ restore config progress

do not switch off device during flash update

total :  8%

## Restart

There are 2 options for you to choose from before restarting the your 8200N device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.



The screenshot shows the 'Configuration' page with a 'Restart' section. It includes a warning message, two radio button options, and a 'Restart' button.

**Configuration**

▼ Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings

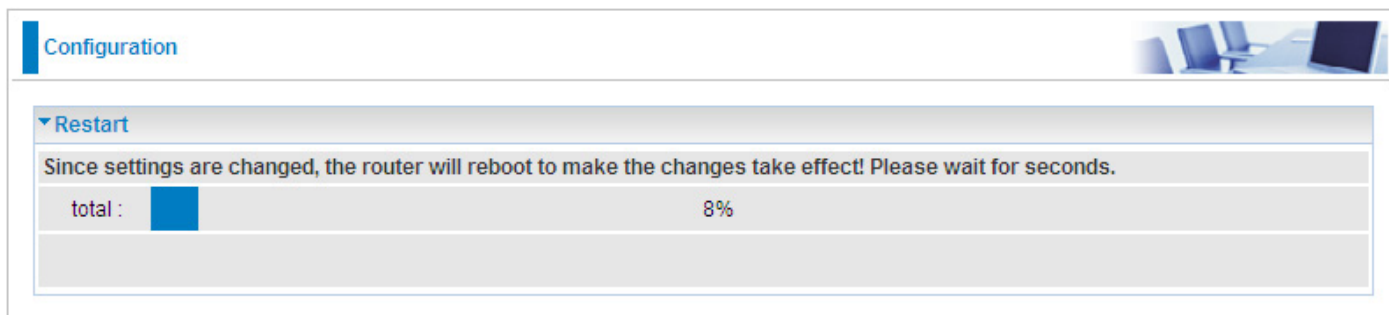
☒ Current Settings

Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

Click Restart with option Current Settings to reboot your router (and restore your last saved configuration).

After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.



The screenshot shows the 'Configuration' page with a 'Restart' section. It includes a warning message and a progress bar.

**Configuration**

▼ Restart

Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.

total :  8%

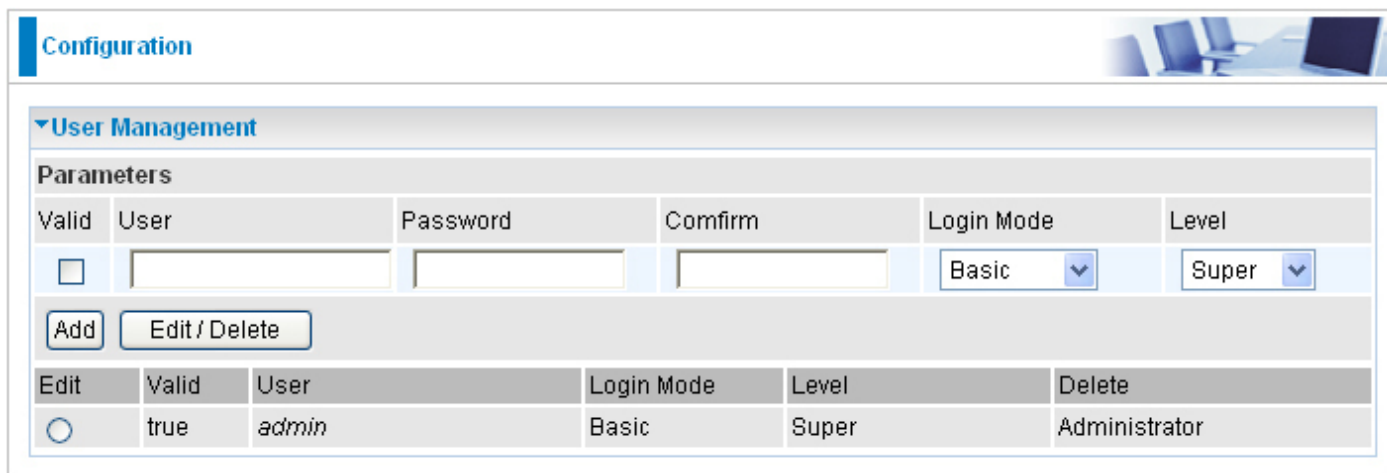
You may also reset your router to factory settings by holding the small Reset pinhole button more than 1 second on the back of your router.



## User Management

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system.

This feature allows you to set up multiple user accounts which contains a unique password of its own. In addition, you can also edit any existing user accounts or add new users to allow access to the device configuration interface.



The screenshot shows the 'Configuration' tab with the 'User Management' section expanded. Under 'Parameters', there are input fields for 'Valid' (checkbox), 'User', 'Password', 'Confirm', 'Login Mode' (dropdown), and 'Level' (dropdown). The 'Add' button is highlighted. Below the parameters, there is a table with columns: Edit, Valid, User, Login Mode, Level, and Delete. The table contains one row for the 'admin' user.

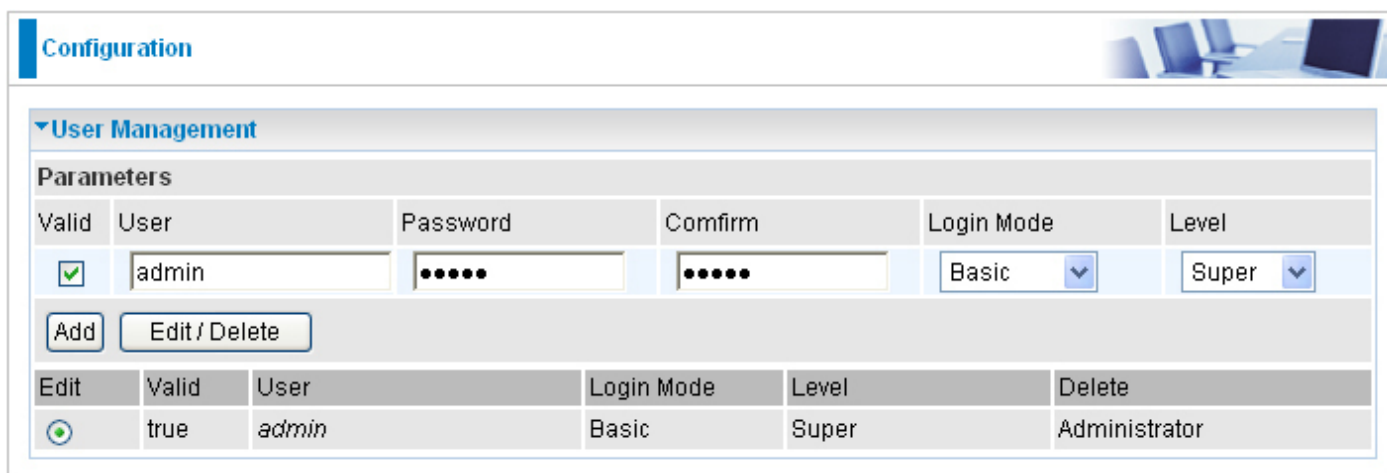
Valid	User	Password	Confirm	Login Mode	Level
<input type="checkbox"/>				Basic	Super

Edit	Valid	User	Login Mode	Level	Delete
<input type="radio"/>	true	admin	Basic	Super	Administrator

### Edit Account Information

You can change the informations of any account whether the account is active or valid.

1. To edit an account, click on the Edit radio button of the account you want to edit. Once selected, all information of that account will be displayed.
2. Delete the information to be edited and replace it with the new one.



The screenshot shows the 'Configuration' tab with the 'User Management' section expanded. Under 'Parameters', the 'Valid' checkbox is checked. The 'Add' button is highlighted. Below the parameters, there is a table with columns: Edit, Valid, User, Login Mode, Level, and Delete. The table contains one row for the 'admin' user.

Valid	User	Password	Confirm	Login Mode	Level
<input checked="" type="checkbox"/>	admin	.....	.....	Basic	Super

Edit	Valid	User	Login Mode	Level	Delete
<input checked="" type="radio"/>	true	admin	Basic	Super	Administrator

3. When it is done, simply click on the Edit/Delete button to save your changes.

**Note:** It is highly recommended that you change the password immediately to prevent security breach to your GUI.

### **Add an account**

1. Check the Valid checkbox, fill in all the information: User name, Comment (optional), Password, Confirm Password.
2. When it is done, click the Add button.

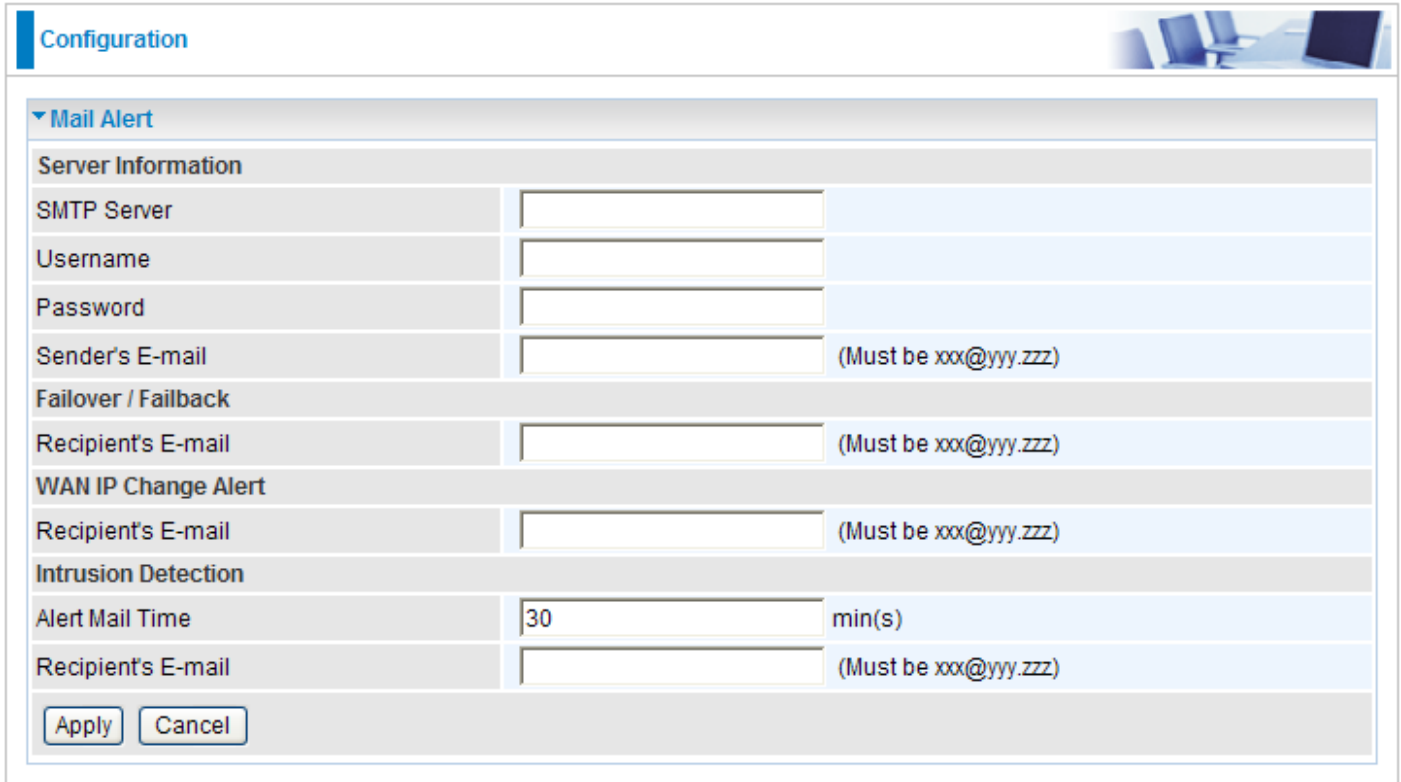
### **Delete a User Account**

1. Check the Delete checkbox of the account you want to delete.
2. Then click the Edit/Delete to confirm the deletion.

***Note: You can delete any user account except for the default admin account. Thus there is no delete radio button available for this account.***

## Mail Alert

Mail Alert allows administrator to receive notifications from the router through email about important events that is occurring in real time. This allows administrator to be able to take immediate actions to counteract any possible hacking or to restore the router to its original status should any failover / failback ever occurs.



**Configuration**

**Mail Alert**

**Server Information**

SMTP Server

Username

Password

Sender's E-mail  (Must be xxx@yyy.zzz)

**Failover / Failback**

Recipient's E-mail  (Must be xxx@yyy.zzz)

**WAN IP Change Alert**

Recipient's E-mail  (Must be xxx@yyy.zzz)

**Intrusion Detection**

Alert Mail Time  min(s)

Recipient's E-mail  (Must be xxx@yyy.zzz)

### Server Information

**SMTP Server:** Enter the SMTP (mail) server address.

**Username:** Enter the username of your SMTP server.

**Password:** Enter the password associated with the username.

**Sender's E-mail:** Enter the email address you wish to send the mail alert email to.

### Failover / Failback

**Recipient's E-mail:** Enter the email address you wish to send the Failover / Failback email to.

### WAN IP Change Alert

**Recipient's E-mail:** Enter the email address you wish to send the WAN IP Change email to.

### Intrusion Detection

**Alert Mail Time:** Set the time for sending the Alert mail.

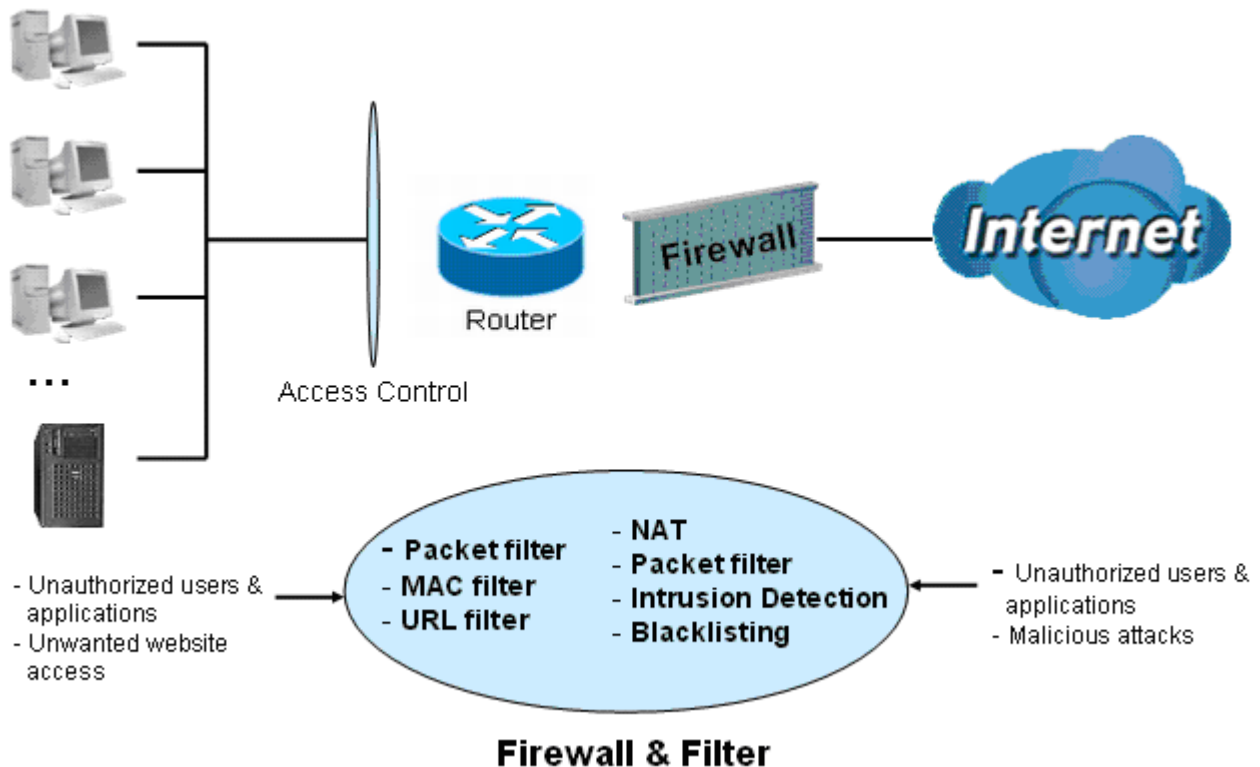
**Recipient's E-mail:** Enter the email address you wish to send the Intrusion Detection email to.

Click Apply to confirm the settings.

# Firewall

## Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the WAN configuration section for more details on NAT.



**Firewall:** Prevents access from outside your network.

**NAT natural firewall:** This masks LAN users' IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

**Firewall Security and Policy (General Settings):** Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

**Intrusion Detection:** Enable Intrusion Detection to detect, prevent, and log malicious attacks.

**MAC Filter rules:** Prevents unauthorized computers accessing the Internet.

**URL Filter:** Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following items appears in the Firewall section below: [Packet Filter](#), [MAC Filter](#), [Intrusion Detection](#), [Block WAN PING](#) and [URL Filter](#).

## Packet Filter

Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “or” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

**Configuration**

**▼ Packet Filter**

**Parameters**

Rule Name	<input type="text"/>	<< --select--	▼ (type or select from listbox)
Internal IP Address	<input type="text"/>	~	<input type="text"/>
External IP Address	<input type="text"/>	~	<input type="text"/>
Protocol	TCP ▼		Action forward ▼
Internal Port	<input type="text"/>	~	<input type="text"/>
External Port	<input type="text"/>	~	<input type="text"/>
Direction	outgoing ▼		Time Schedule Always On ▼
		Log	<input type="checkbox"/>

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
			External IP Address		External Port				
		Default	Any	Any	Any	outgoing	forward	Always On	
			Any		Any				

**Rule Name:** User defined description for entry identification. The maximum name length is 32 characters, and then can choose an application that they want from the listbox.

**Internal IP Address / External IP Address:** This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Input the range you want to filter out. If you leave these four fields empty or enter 0.0.0.0, it means any IP address.

**Protocol:** Specify the packet type (TCP, UDP, TCP/UDP) that the rule applies to. Select TCP if you wish to search for the connection-based application service on the remote server using the port number. Or select UDP if you want to search for the connectionless application service on the remote server using the port number.

**Action:** If a packet matches this filter rule, forward (allows the packets to pass) or drop (disallow the packets to pass) this packet.

**Internal Port:** This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set the range from 1 to 65535. It is recommended that this option be configured by an advanced user.

**External Port:** This is the Port or Port Range that defines the application.

**Direction:** Determine whether the rule is for outgoing packets or for incoming packets.

**Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

**Log:** Check the checking box if you wish to generate logs when the filter rule is applied to a packet.

**Add:** Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

**Edit:** Check Edit next to the item you wish to edit, and then change parameters as desired. Complete it by press “Edit/Delete”.

**Delete:** Check Edit next to the item you wish to delete, and press “Edit/Delete” to remove this rule.

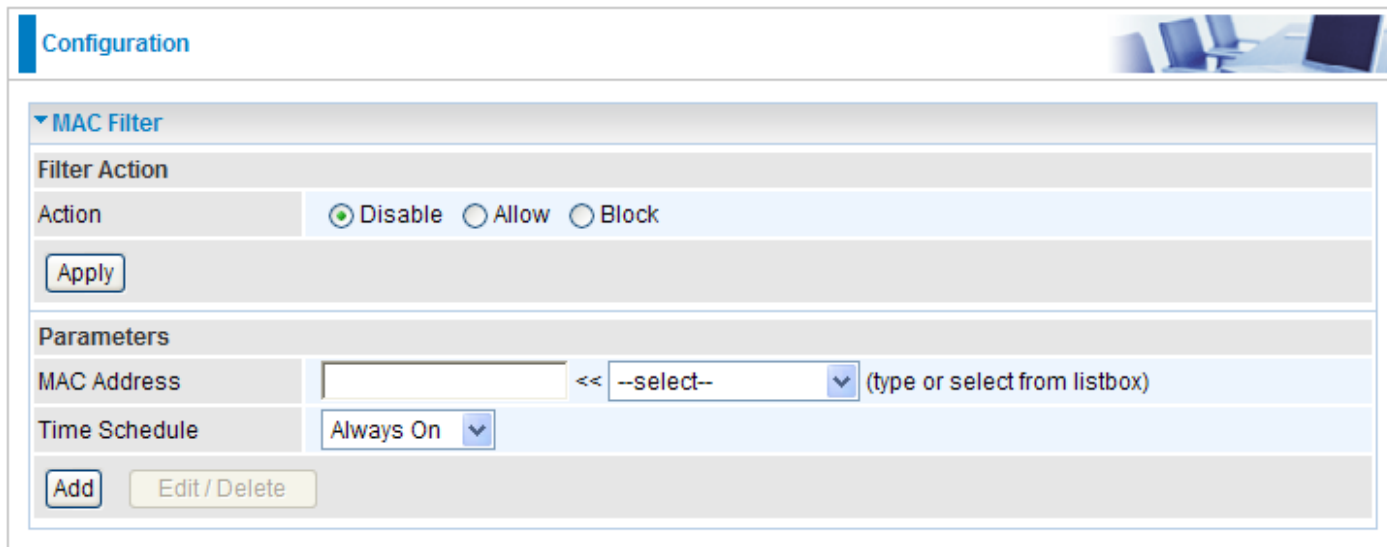
**Order:** Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press “Reorder” to save the new priority.

Edit	Order	Rule Name	Internal IP Address	Protocol	Internal Port	Action	Direction	Delete
			External IP Address		External Port			
<input type="radio"/>	↓	FTP	Any	TCP	Any	outgoing	drop	<input type="checkbox"/>
			Any		21 ~ 21			
<input type="radio"/>	↑	HTTP	Any	TCP	Any	outgoing	drop	<input type="checkbox"/>
			Any		80 ~ 80			
		Default	Any	Any	Any	outgoing	forward	
			Any		Any			

## MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules, you can add the filter rules to meet your requirements.



Configuration

▼ MAC Filter

Filter Action

Action ☒ Disable ☐ Allow ☐ Block

Apply

Parameters

MAC Address  << --select-- (type or select from listbox)

Time Schedule Always On

Add Edit / Delete

The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

### Filter Action

**Action:** Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

### Server Information

**MAC Address:** Enter the MAC addresses you wish to have the filter rule applies.

## Intrusion Detection

The router Intrusion Detection System (IDS) is used to detect hacker's attack and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Configuration

▼Intrusion Detection

Parameters

Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Maximum TCP Open Handshaking Count	<input type="text" value="100"/> per second
Maximum Ping Count	<input type="text" value="15"/> per second
Maximum ICMP Count	<input type="text" value="100"/> per second
Log	<input type="checkbox"/>

**Intrusion Detection:** Check Enable if you wish to detect intruders accessing your computer without permission.

**Maximum TCP Open Handshaking Count:** This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

**Maximum Ping Count:** This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

**Maximum ICMP Count:** This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

**Log:** Check Log if you wish to generate logs when the filter rule is applied to the Intrusion Detection.

Click Apply to confirm the settings.



**Table: Hacker attack types recognized by the IDS**

<b>Intrusion Name</b>	<b>Detect Parameter</b>	<b>Blacklist</b>	<b>Type of Block Duration</b>	<b>Drop Packet</b>	<b>Show Log</b>
<b>Ascend Kill</b>	Ascend Kill data	Src IP	DoS	Yes	Yes
<b>WinNuke</b>	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
<b>Smurf</b>	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
<b>Land attack</b>	SrcIP = DstIP			Yes	Yes
<b>Echo/CharGen Scan</b>	UDP Echo Port and CharGen Port			Yes	Yes
<b>Echo Scan</b>	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
<b>CharGen Scan</b>	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
<b>X'mas Tree Scan</b>	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
<b>IMAP SYN/FIN Scan</b>	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
<b>SYN/FIN/RST/ACK Scan</b>	TCP No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
<b>Net Bus Scan</b>	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
<b>Back Orifice Scan</b>	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
<b>SYN Flood</b>	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
<b>ICMP Flood</b>	Max ICMP Count (Default 100 c/sec)				Yes
<b>ICMP Echo</b>	Max PING Count (Default 15 c/sec)				Yes

**Src IP:** Source IP

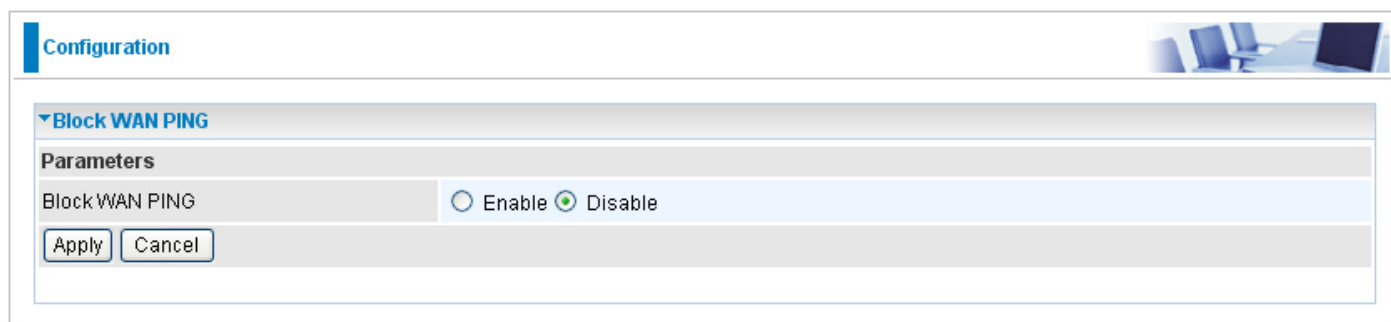
**Src Port:** Source Port

**Dst Port:** Destination Port

**Dst IP:** Destination IP

## Block WAN Ping

This feature is to be enabled when you want the public WAN IP address on your router not to respond to any ping command.



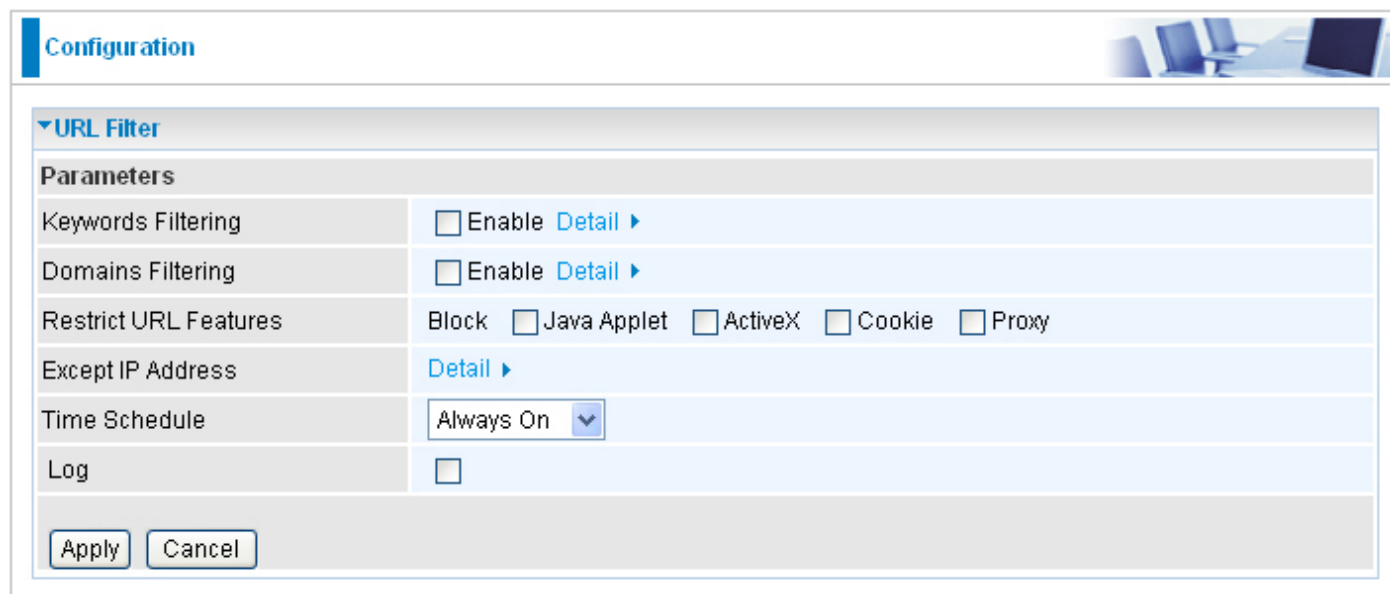
The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Block WAN PING' is expanded. Under this section, there is a 'Parameters' area. The 'Block WAN PING' parameter is set to 'Disable', indicated by a selected radio button. Below the parameter, there are 'Apply' and 'Cancel' buttons. A small image of a router is visible in the top right corner of the configuration area.

Configuration	
Block WAN PING	
Parameters	
Block WAN PING	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

This feature is disabled by default. To activate the Block WAN PING feature, check the Enable box then click the Apply button.

## URL Filter

URL (Uniform Resource Locator) (e.g. an address in the form of <http://www.abcde.com> or <http://www.example.com>) filter rule allows you to prevent users on your network from accessing specific websites defined by their URL. There are no predefined URL filter rules, therefore you can add filter rules to meet your requirements.



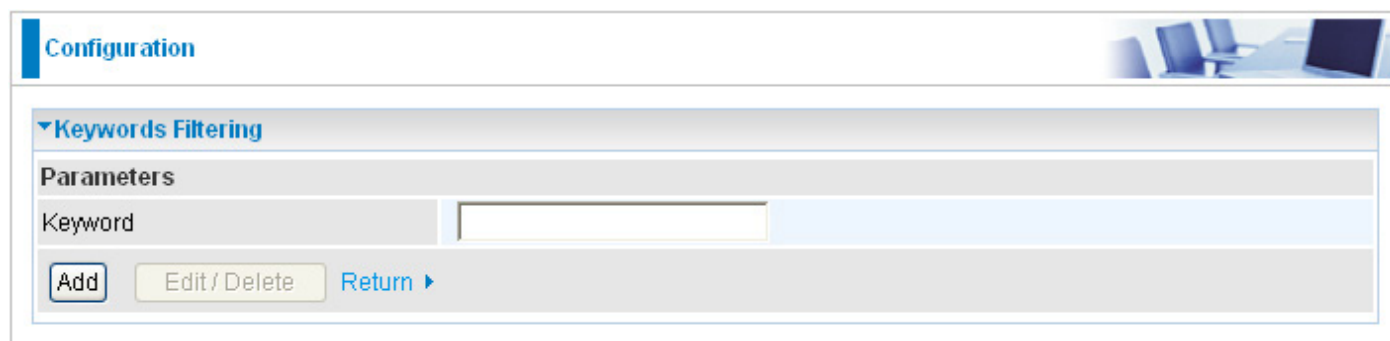
The screenshot shows the 'Configuration' window for the 'URL Filter'. It has a 'Parameters' section with the following settings:

Parameter	Value
Keywords Filtering	<input type="checkbox"/> Enable <a href="#">Detail ▶</a>
Domains Filtering	<input type="checkbox"/> Enable <a href="#">Detail ▶</a>
Restrict URL Features	Block <input type="checkbox"/> Java Applet <input type="checkbox"/> ActiveX <input type="checkbox"/> Cookie <input type="checkbox"/> Proxy
Except IP Address	<a href="#">Detail ▶</a>
Time Schedule	Always On ▼
Log	<input type="checkbox"/>

At the bottom are 'Apply' and 'Cancel' buttons.

**Keywords Filtering:** Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is <http://www.abc.com/abcde.html>, it will be dropped as the keyword “abcde” occurs in the URL.



The screenshot shows the 'Configuration' window for 'Keywords Filtering'. It has a 'Parameters' section with a 'Keyword' text input field. Below the input field are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

**Domains Filtering:** This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped.
3. If the packet does not match either of the above two items, it is sent to the remote web server.

4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to [www.google.com.au](http://www.google.com.au), enter “[www.google](http://www.google.com)” or “[www.google.com](http://www.google.com)”.

Configuration

▼ Domains Filtering

Parameters

Domain Name

Type

Forbidden Domain ▼

Add

Edit / Delete

Return ▶

Forbidden Domain

Edit	Domain Name	Delete
<input type="radio"/>	www.google	<input type="checkbox"/>

Trusted Domain

Edit	Domain Name	Delete
<input type="radio"/>	www.abc	<input type="checkbox"/>

**Restrict URL Features:** This function enhances the restriction to your URL rules.

**Block Java Applet:** Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.

**Block ActiveX:** Blocks ActiveX.

**Block Cookies:** Blocks Cookies.

**Block Proxy:** Blocks Proxy.

**Except IP Address:** The except IP address list.

Configuration

▼ Except IP Address

Parameters

Internal IP Address

~

Add

Edit / Delete

Return ▶

**Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

**Log:** Check this checking box if you wish to generate logs when the filter rule is applied to the URL Filter.

Click Apply to confirm the settings.

## QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.

**Configuration**

**QoS**

**Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100%    Downstream (WAN to LAN) : 100%**

**Parameters**

Application	<input type="text"/>	Direction	LAN to WAN ▾		
Protocol	Any ▾	DSCP Marking	Disable ▾		
Rate Type	Guaranteed (Minimum) ▾	Ratio	<input type="text"/> %	Priority	Normal ▾
Internal IP Address	<input type="text"/> ~ <input type="text"/>	Internal Port	<input type="text"/> ~ <input type="text"/>		
External IP Address	<input type="text"/> ~ <input type="text"/>	External Port	<input type="text"/> ~ <input type="text"/>		
Time Schedule	Always On ▾				

After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

**Application:** Assign a name that identifies the new QoS application rule.

**Direction:** The traffic flow direction to be controlled by the QoS policy. There are two settings to be provided in the Router:

**LAN to WAN:** Control the traffic flow from the local network to the outside world. For example, when you have a FTP server inside the local network and want to have a limited traffic rate controlled by the QoS policy, you need to add a policy with LAN to WAN direction setting.

**WAN to LAN:** Control Traffic flow from the WAN to LAN. (The connection maybe either issued from LAN to WAN or WAN to LAN.)

**Protocol:** Select the supported protocol from the drop down list. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

Any: No protocol type is specified.

TCP

UDP

ICMP

GRE: For PPTP VPN Connections.

**DSCP Marking:** Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value. See [DSCP Mapping Table](#).

**Note:** Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.

DSCP Mapping Table

DSCP Mapping Table	
(Wireless) VDSL Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

**Rate Type:** Two types are provided:

**Limited (Maximum):** Specify a limited data rate for this policy. It is the maximal rate for this policy. As above FTP server example shows, if you want to “throttle” the outgoing FTP speed to 20% of 100M and limit to it, please choose this type.

**Guaranteed (Minimum):** Specify a minimal data rate for this policy. For example, if you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth, please choose this type. Then, if the available bandwidth is not used, it will be given to this policy by following priority assignment.

**Ratio:** Assign the data ratio for this policy to be controlled. For examples, when we want to allow only 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server, we can specify here with data ratio = 20. If you have VDSL LINE with 100M/bps.rate, the estimated data rate, in kbps, for this rule is  $20\% \times 100 \times 0.9 = 20\text{Mbps}$ . (For 0.9 is an estimated factor for the effective data transfer rate for a VDSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

**Priority:** The priority given to each policy/application. You may adjust this setting to fit your policy / application. For examples, you are allowed to specify two different QoS policies for different applications. Both applications need minimal or higher bandwidth, besides the assigned one, if there is any available/non-used one available, you can specify which application can have higher priority by acquiring the non-used bandwidth.

**High**

**Normal:** The default is set to normal.

**Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

**Internal IP Address:** The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

**Internal Port:** The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

**External IP Address:** The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

**External Ports:** The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

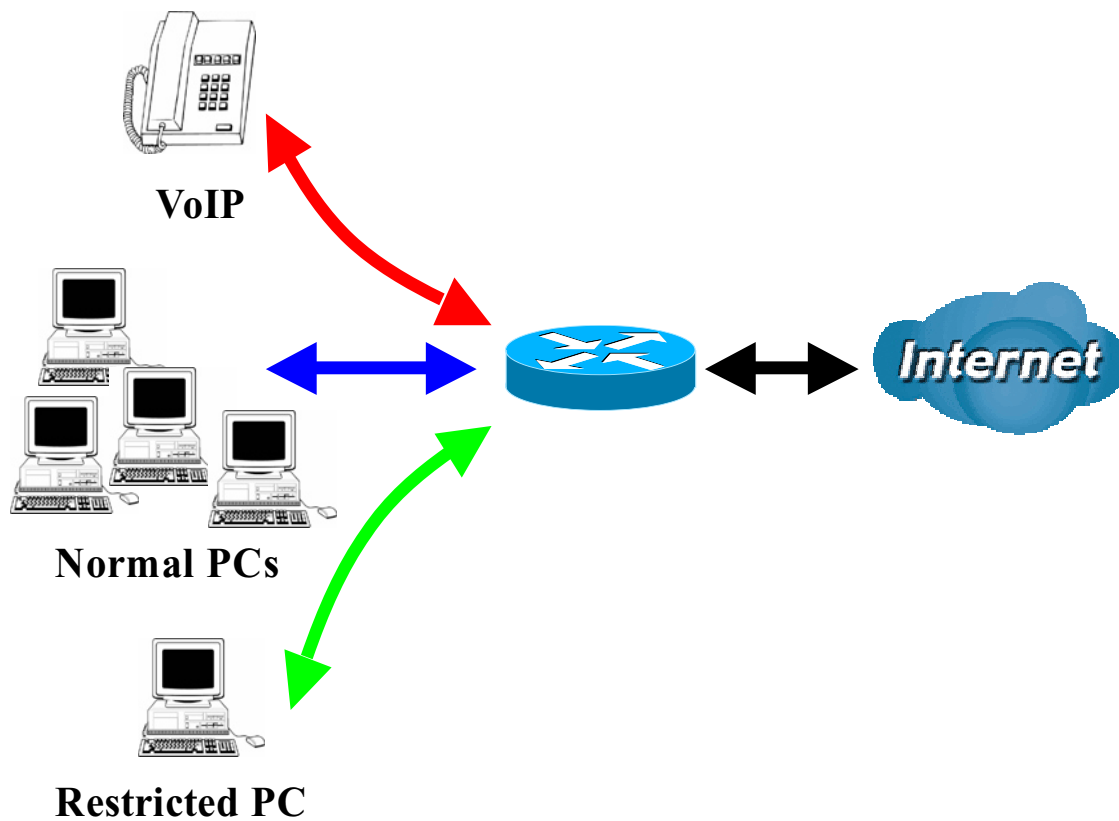
**Time Schedule:** Scheduling your prioritization policy.

Remember clicking Add to save your settings.



## Example: QoS for your Network

### Connection Diagram



Application	IP / Ports	Control Flow	Data Rate	Time Schedule
VoIP user	192.168.0.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with DSCP marking Class 1 Gold Service.	Always
FTP Server	192.168.0.100	Incoming & Outgoing	Outgoing :minimal 30% data rate. Incoming :minimal 30% data rate. Both with low priority for non-used bandwidth.	Only during working hours 9:00 to 17:00 Monday to Friday
HTTP Web user	80	Incoming & Outgoing	Outgoing : limited 20% data rate. Incoming : limited 30% data rate.	Always

## Example: QoS Setup

**Configuration**

**QoS**

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 45%    Downstream (WAN to LAN) : 65%

Parameters

Application	<input type="text"/>	Direction	LAN to WAN ▾		
Protocol	Any ▾	DSCP Marking	Disable ▾		
Rate Type	Guaranteed (Minimum) ▾	Ratio	<input type="text"/> %	Priority	Normal ▾
Internal IP Address	<input type="text"/> ~ <input type="text"/>	Internal Port	<input type="text"/> ~ <input type="text"/>		
External IP Address	<input type="text"/> ~ <input type="text"/>	External Port	<input type="text"/> ~ <input type="text"/>		
Time Schedule	Always On ▾				

Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
<input type="radio"/>	VOIP	LAN to WAN	Guaranteed	20%	Always On	<input type="checkbox"/>
<input type="radio"/>	FTP Server (OUT)	LAN to WAN	Guaranteed	15%	TimeSlot1	<input type="checkbox"/>
<input type="radio"/>	FTP Server (IN)	WAN to LAN	Guaranteed	15%	TimeSlot1	<input type="checkbox"/>
<input type="radio"/>	HTTP Borwing (OUT)	LAN to WAN	Limited	20%	TimeSlot2	<input type="checkbox"/>
<input type="radio"/>	HTTP Borwing (IN)	WAN to LAN	Limited	20%	TimeSlot2	<input type="checkbox"/>

### VoIP application

Voice is latency-sensitive application. Most VoIP devices are used SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

## Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

### Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table below). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: <http://www.iana.org/assignments/port-numbers>.

For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at <http://www.billion.com>.

### Well-known and Registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	Real Audio

## Port Mapping

Since NAT acts as a “natural” Internet firewall, your router protects your network from accessed by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request the router for a specified port is received, it is forwarded to the corresponding internal server.

Configuration

Port Mapping

Parameters

Application

<< --select--

(type or select from listbox)

Protocol

TCP

External Port

~

Internal IP Address

<< --select--

(type or select from listbox)

Internal Port

Time Schedule

Always On

Add

Edit / Delete

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
<input type="radio"/>	FTP	TCP	21~21	192.168.1.25	Any	Always On	<input type="checkbox"/>
<input type="radio"/>	HTTP	TCP	80~80	192.168.1.2	Any	Always On	<input type="checkbox"/>

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by a particular application. Most applications use TCP or UDP, however you may also specify other protocols using the drop-down Protocol menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

**Application:** Select the service you wish to configure.

**Protocol:** A protocol is automatically applied when an Application is selected from the listbox or you may select a protocol type which you want. The protocol used to be determined by a particular application. Most applications will use TCP or UDP.

**External Port & Internal Port:** Enter the public port number & range you wish to configure.

**Internal IP Address:** Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

**Time Schedule:** Scheduling your prioritization policy.

**Add:** Click to add a new virtual server rule. Click again and the next figure appears.

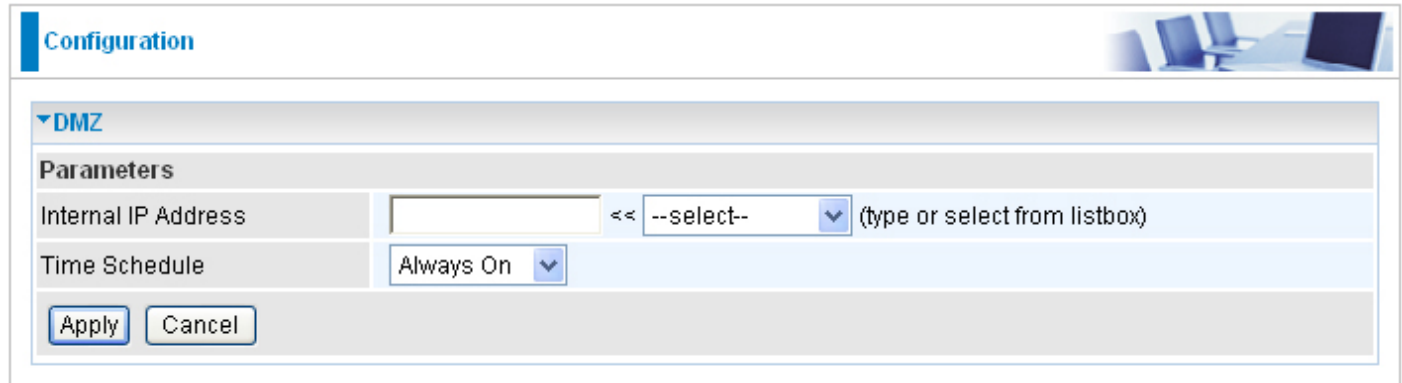
**Edit:** Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the Edit/Delete button to apply the changes.

**Delete:** To remove a port mapping application, check the Delete box of the selected application then click the Edit/Delete button.

## DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host.

***Cautious: This Local computer exposing to the Internet may face various security risks.***



The screenshot shows a 'Configuration' window with a 'DMZ' section expanded. Under 'Parameters', there are two fields: 'Internal IP Address' with an empty text box and a dropdown menu set to '--select--' (with a note '(type or select from listbox)'), and 'Time Schedule' with a dropdown menu set to 'Always On'. At the bottom are 'Apply' and 'Cancel' buttons.

**Time Schedule:** Scheduling your prioritization policy.

Click Apply to confirm the settings.



### Attention

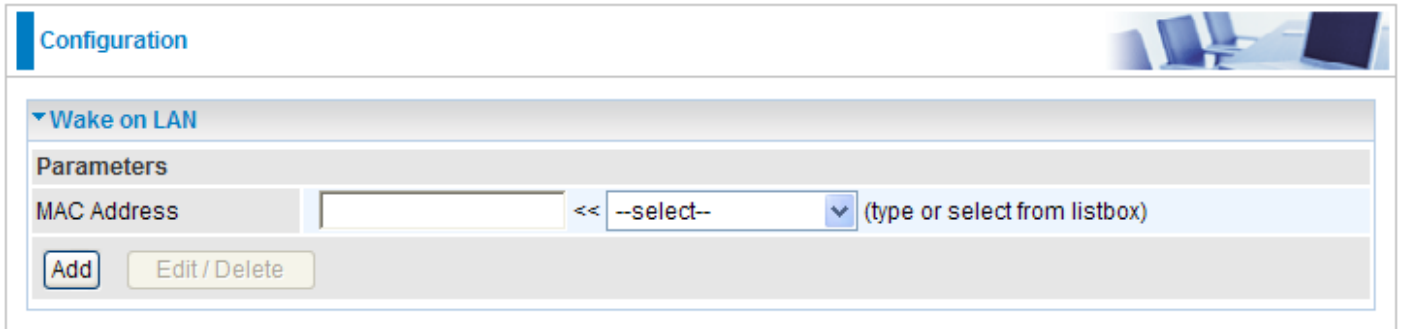
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP addresses to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in



Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore advised to use specific Virtual Server entries just for those ports that your applications require.

## Wake on LAN

WOL allows the router to set a command to turn on a particular computer that can support this feature.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Wake on LAN' section is expanded. Under the 'Parameters' heading, there is a 'MAC Address' label followed by a text input field. To the right of the input field is a dropdown menu with '<< --select--' and a downward arrow. Further right is the text '(type or select from listbox)'. At the bottom of the section, there are two buttons: 'Add' and 'Edit / Delete'.

Click Add to save the setting.

**Edit:** Check the Edit radio button to display the parameter of the selected entry, then after changing the parameters click the "Edit/Delete" button to apply the changes.

**Delete:** To remove a static route entry, check the Delete box of the selected entry then click the "Edit/Delete" button.



# Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to Time Zone for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Configuration

Time Schedule

Parameters

Name

Day in a week

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Start Time

08 : 00

End Time

18 : 00

Edit / Clear

Edit	Name	Day in a week	Start Time	End Time	Clear
<input type="radio"/>	TimeSlot1	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot2	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot3	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot4	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot5	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot6	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot7	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot8	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot9	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot10	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot11	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot12	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot13	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot14	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot15	smtwtfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot16	smtwtfs	08:00	18:00	<input type="checkbox"/>

**Name:** A user-define description to identify this time portfolio.

**Day in a week:** The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

**Start Time:** The default is set at 8:00 AM. You may specify the start time of the schedule.

**End Time:** The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

Click the Edit/Clear button to save your changes.

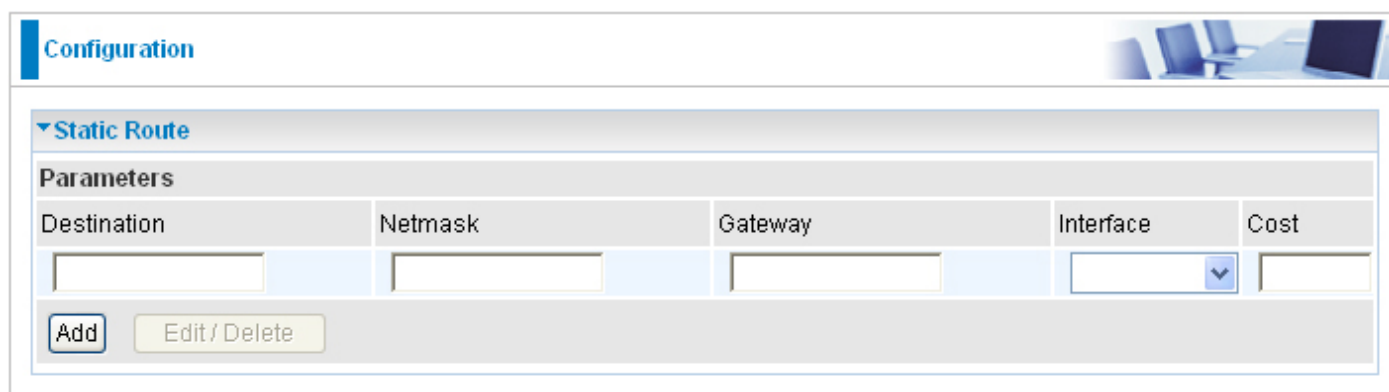
## Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the Advanced section: [Static Route](#), [Static ARP](#), [Dynamic DNS](#), [VLAN](#), [Device Management](#), [IGMP](#), [SNMP Access Control](#), [TR-069](#) and [Remote Access](#).

### Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed to.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Static Route' section is expanded. Under 'Static Route', there is a 'Parameters' section. This section contains a table with five columns: 'Destination', 'Netmask', 'Gateway', 'Interface', and 'Cost'. Each column has a corresponding input field. The 'Interface' field is a dropdown menu. Below the table, there are two buttons: 'Add' and 'Edit / Delete'.

Destination	Netmask	Gateway	Interface	Cost
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>

**Destination:** Enter the destination IP where the traffic is to be forwarded.

**Netmask:** Enter the netmask of the destination.

**Gateway:** Enter the gateway address for the traffic.

**Interface:** Select an appropriate interface for the new routing rule from the drop down menu.

**Cost:** This is the same meaning as Hop and represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535; usually be left at 1.

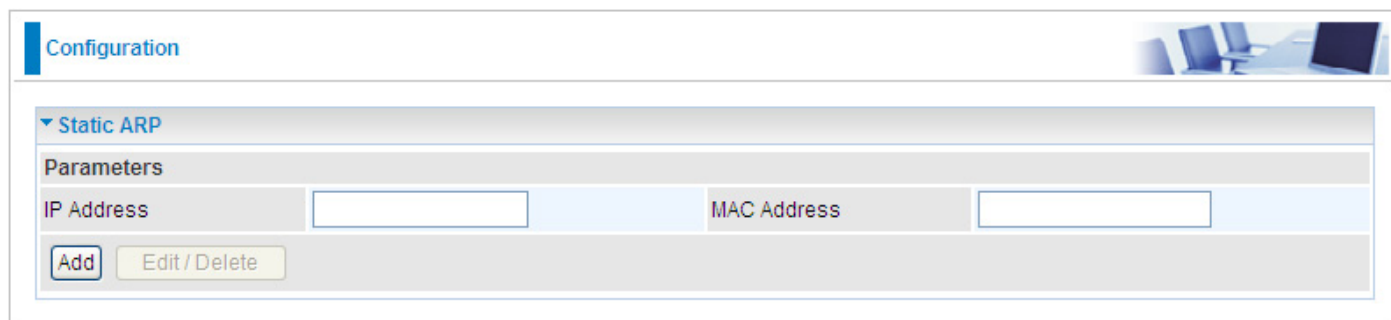
Click Add to confirm the settings.

**Edit:** Check the Edit radio button to display the parameter of the selected rule, then after changing the parameters click the "Edit/Delete" button to apply the changes.

**Delete:** To remove a static route entry, check the Delete box of the selected rule then click the "Edit/Delete" button.

## Static ARP

This feature allows you to map the layer-2 MAC (Media Access Control) address that corresponds to the layer-3 IP address of the device.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static ARP' is expanded. Under this section, there is a 'Parameters' area. This area contains two input fields: 'IP Address' and 'MAC Address'. Below these fields are two buttons: 'Add' and 'Edit / Delete'.

**IP Address:** Enter the IP of the device that the corresponding MAC address will be mapped to.

**MAC Address:** Enter the MAC address that corresponds to the IP address of the device.

Click Add to confirm the settings.

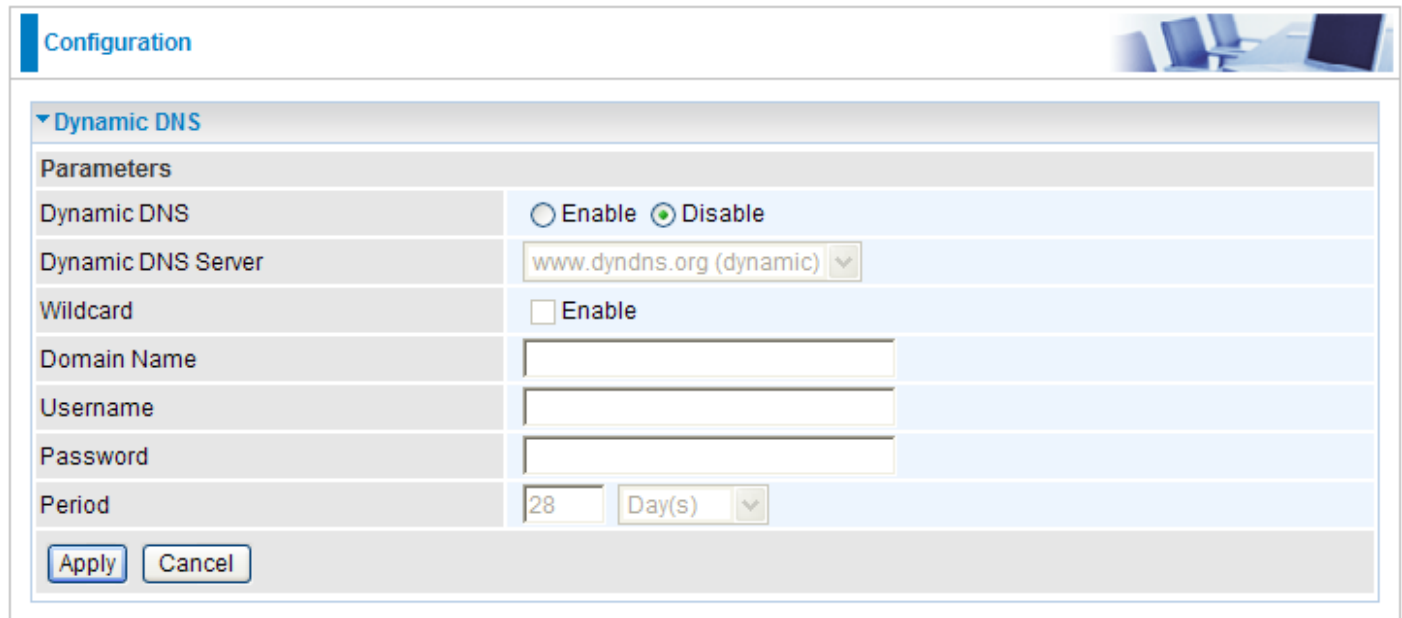
**Edit:** Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.

**Delete:** To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

## Dynamic DNS

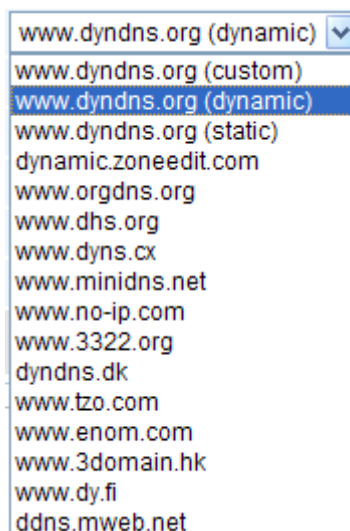
The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful when hosting servers via your WAN connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

You need to first register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>.



**Dynamic DNS:** Default is disabled. Check Enable to enable the Dynamic DNS function and the following fields will be activated and required.

**Dynamic DNS Server:** Select the DDNS service you have registered an account with.



**Wildcard:** When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

**Domain Name, Username and Password:** Enter your registered domain name and your username and password for this service.

**Period:** Enter the length of the period in the blank, you can set the period unit in day, hour or minute.

Click Apply to confirm the settings.

## VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.

**Configuration**

**▼ VLAN**

**Parameters**

VLAN Group Name	VLAN ID	Ethernet Port				WAN Tag
		#1	#2	#3	#4	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/>
LAN Tagging		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

**VLAN Group Name:** Please input VLAN name of this rule.

**VLAN ID:** Please input VLAN ID that will be used for Tagged member port(s).

**Ethernet Port(s):** Please check the interface that you would like to use in this VLAN ID group.

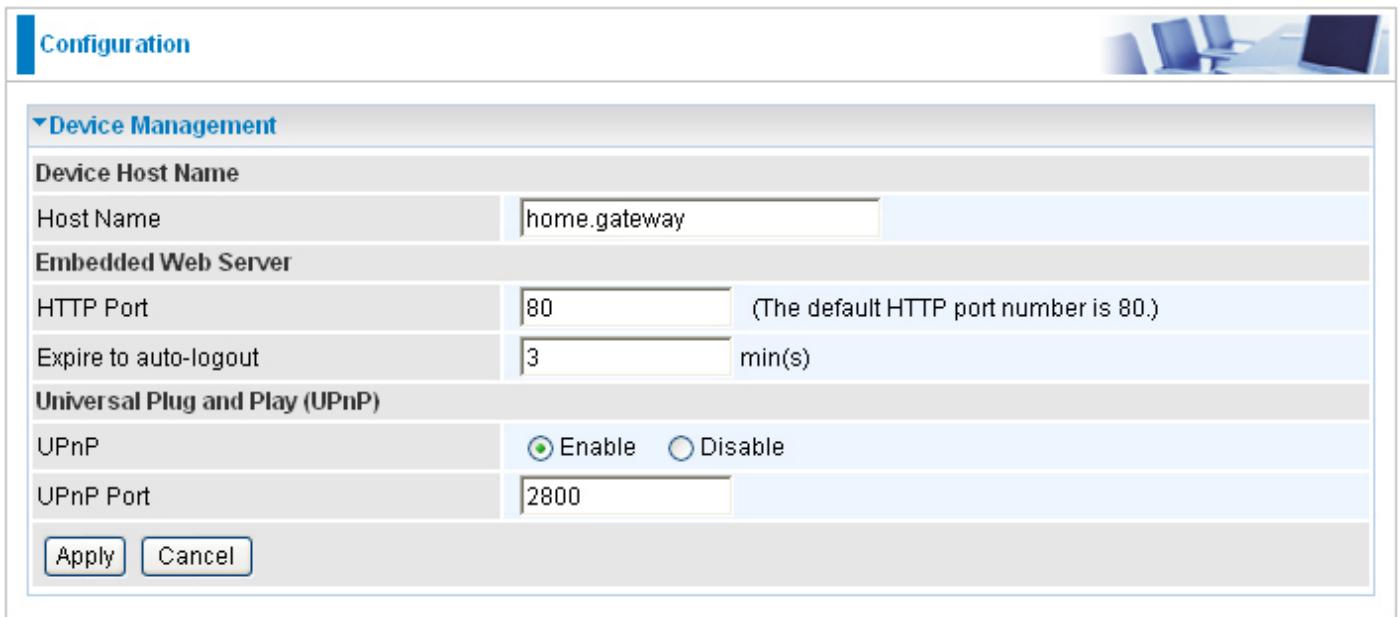
**WAN Tag:** Select the WAN Tag from the drop-down menu to associate the VLAN Group with it. There are 4 options:

- **Untag WAN (NAT):** Outgoing frames without VLAN (Network Address Translation/routing).
- **Tag WAN (Bridge):** Outgoing frames with VLAN (bridging/forwarding) .
- **Untag WAN (Bridge):** Outgoing frames without VLAN (bridging/forwarding).
- **Tag WAN (NAT):** Outgoing frames with VLAN (Network Address Translation/routing).

Click Apply to confirm the settings.

## Device Management

The Device Management advanced configuration settings allows you to control your router's security options and device monitoring features.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Device Management' section is expanded. The 'Device Host Name' section has a text input field containing 'home.gateway'. The 'Embedded Web Server' section has two fields: 'HTTP Port' set to '80' with a note '(The default HTTP port number is 80.)' and 'Expire to auto-logout' set to '3' minutes. The 'Universal Plug and Play (UPnP)' section has two radio buttons: 'Enable' (selected) and 'Disable'. Below these is a 'UPnP Port' field set to '2800'. At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

### Device Host Name

Host Name: Assign it a name.

***(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.***

***Example:***

***Host Name: homegateway ==> Incorrect***

***Host Name: home.gateway or my.home.gateway ==> Correct)***

### Embedded Web Server ( 2 Management IP Accounts)

**HTTP Port:** This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

**Expire to auto-logout:** Specify a time length for the system to auto-logout user from the configuration session.

***Example: User A enters 100 for HTTP port number, specifies 192.168.1.55 for his/hser own IP address, and sets the logout time to 100 minutes. The router will allow User A to access only from the IP address 192.168.1.55 to logon to the Web GUI by typing: http://192.168.1.254:100 in their web browser. After 100 minutes, User A is logged out by the device automatically.***

## **Universal Plug and Play (UPnP)**

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with the feature to control data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems. By letting the application control the required settings and removing the need for the user to control the advanced configuration of their device will make tasks such as port forwarding become easier.

Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UpnP feature. Windows 2000 does not support UPnP.

**Disable:** Check to inactive the router's UPnP functionality.

**Enable:** Check to active the router's UPnP functionality.

**UPnP Port:** Default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports that have been used, you are allowed to change the port number.

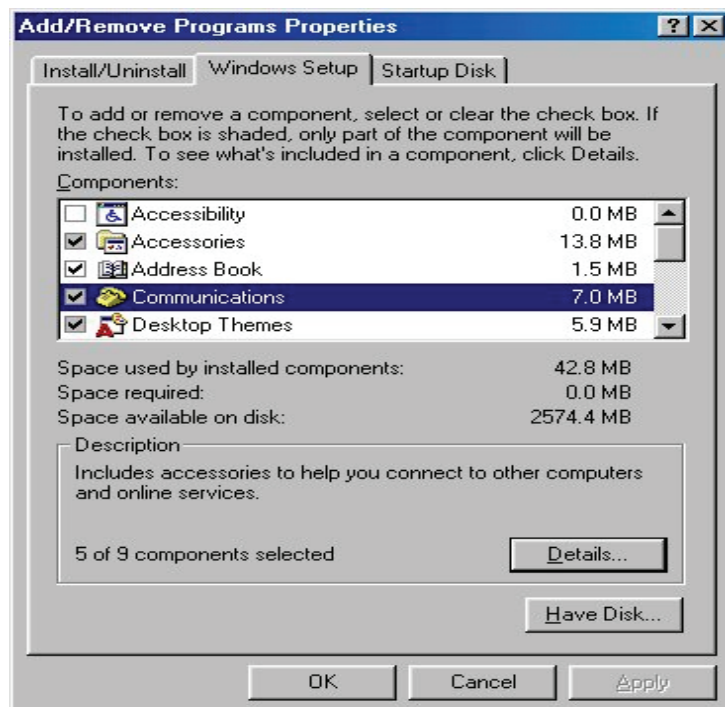
Click Apply to confirm the settings.

## Installing UPnP in Windows Example

### Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.





Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

Step 5: Restart the computer when prompted.

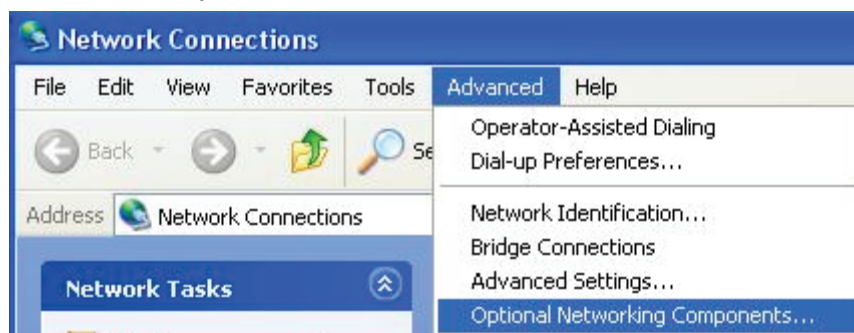
### **Follow the steps below to install the UPnP in Windows XP.**

Step 1: Click Start and Control Panel.

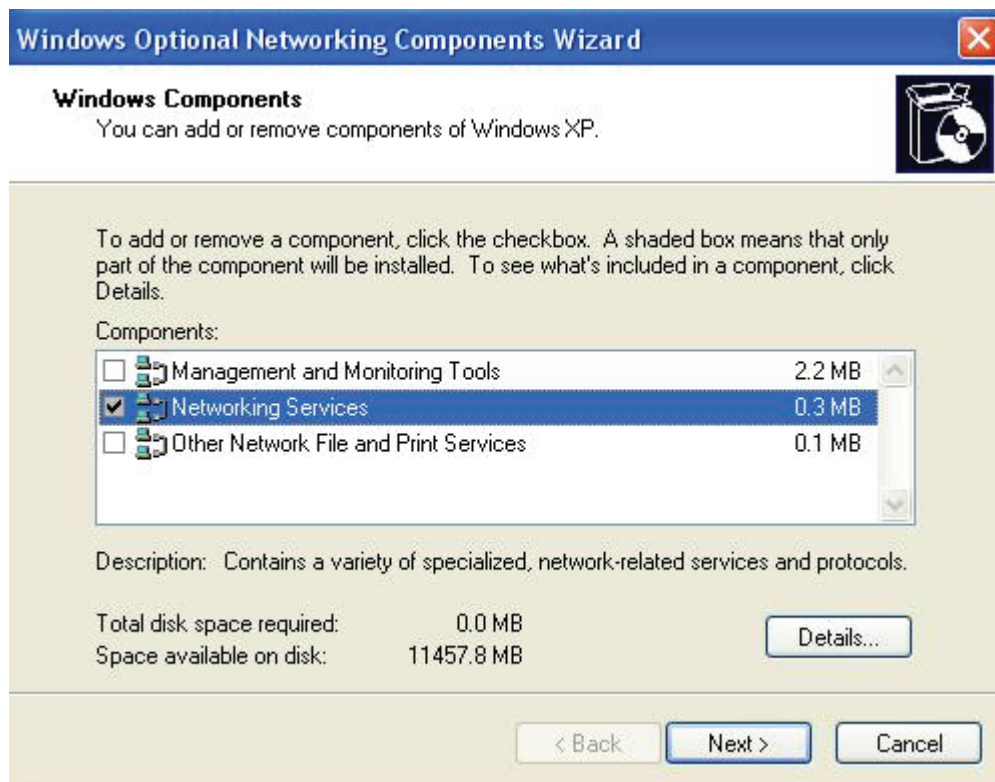
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ....

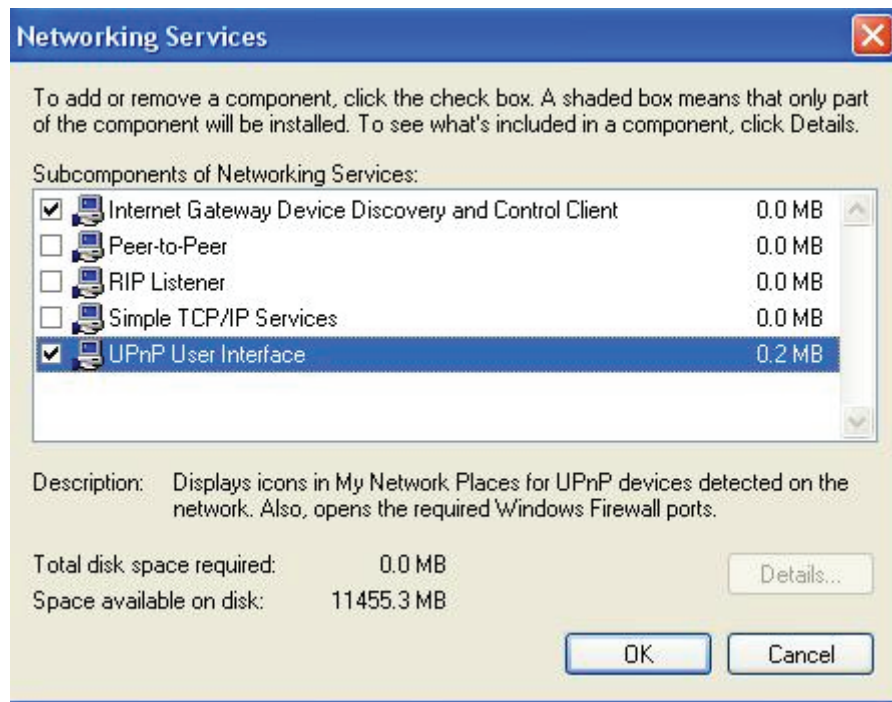
Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.



Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.



## Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

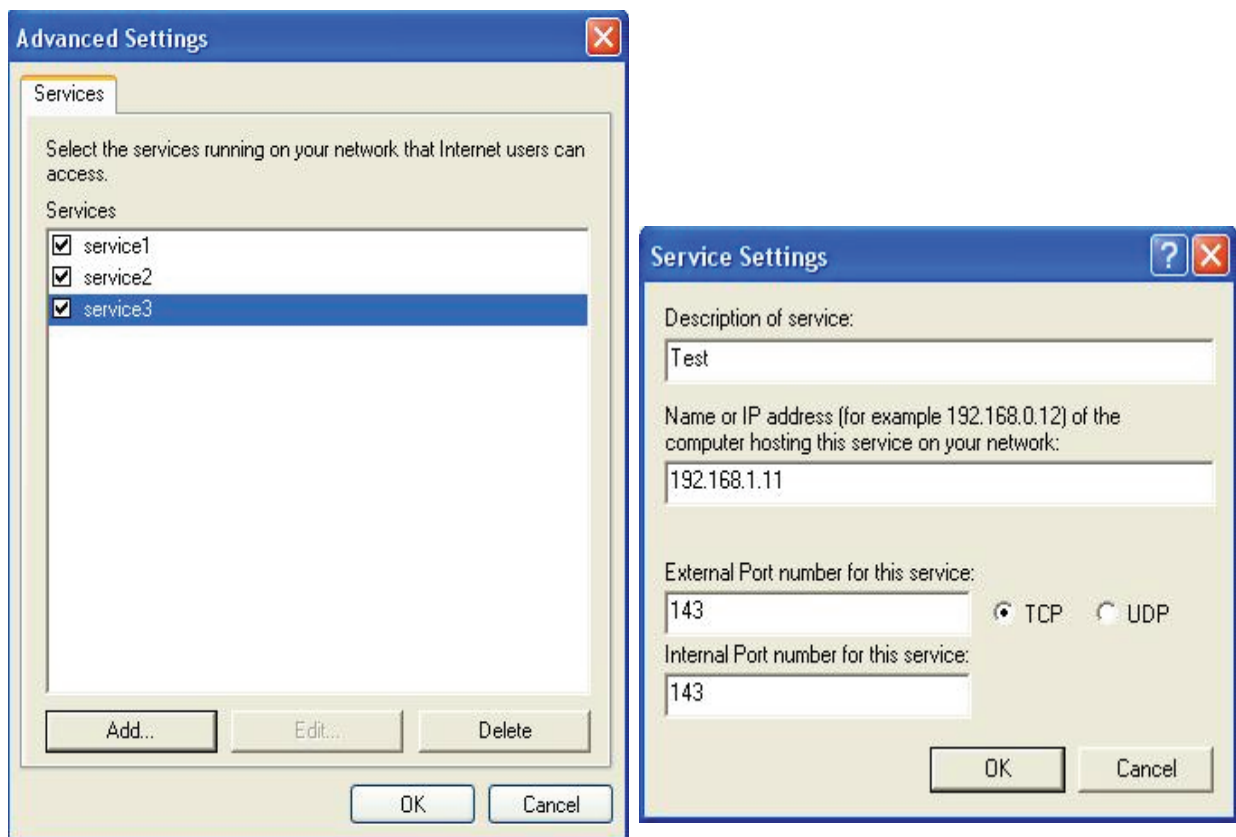
Step 2: Right-click the icon and select Properties.



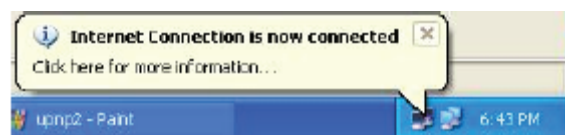
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



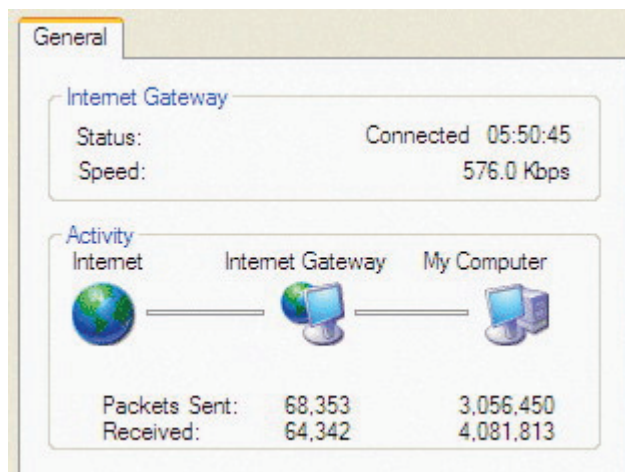
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.



Step 6: Double-click on the icon to display your current Internet connection status.



## Web Configurator Easy Access

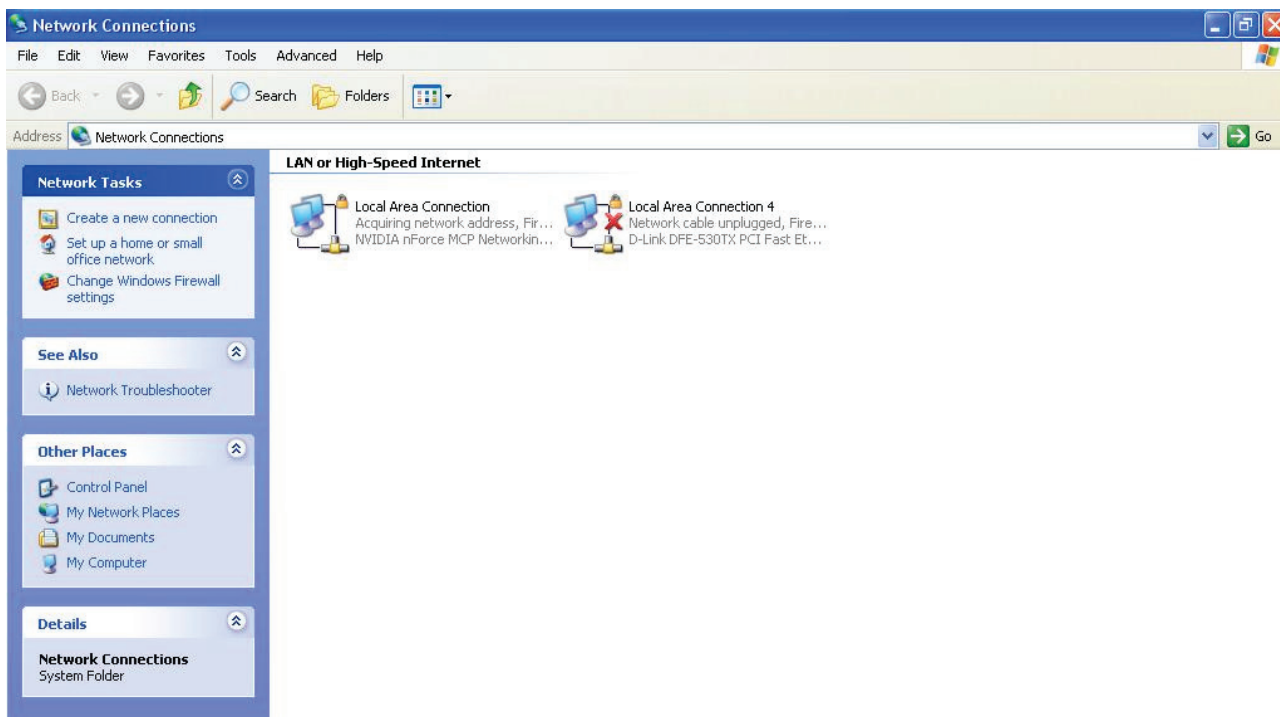
With UPnP, you can access web-based configuration for the BiPAC 8200N without first finding out the IP address of the router. This helps if you do not know the router's IP address.

### Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



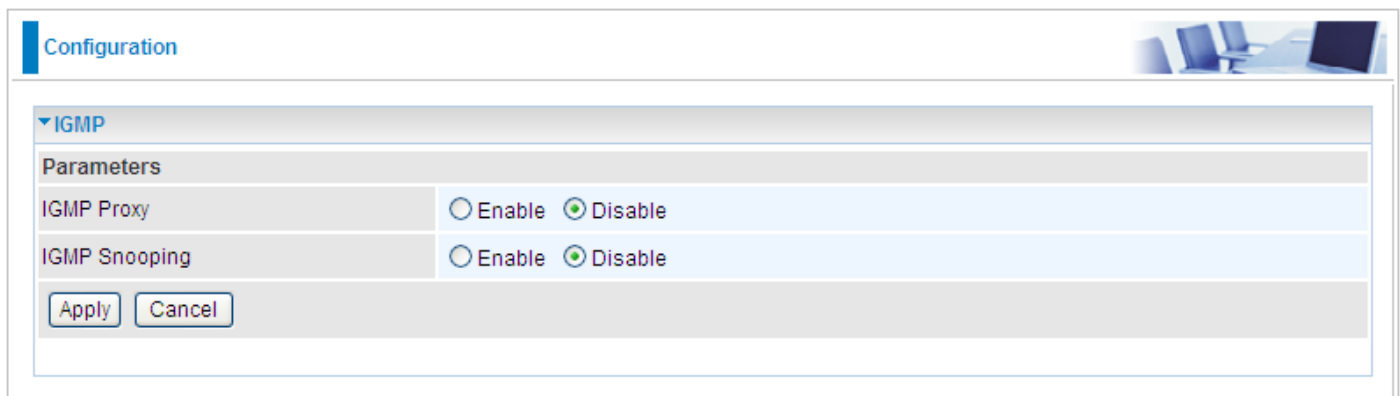
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 8200N and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 8200N and select Properties. A properties window displays basic information about the BiPAC 8200N.

## IGMP

IGMP, known as Internet Group Management Protocol, is used to manage hosts from multicast group.



The screenshot shows a web-based configuration interface for IGMP. At the top, there is a 'Configuration' tab. Below it, the 'IGMP' section is expanded, showing a 'Parameters' table. The table has two rows: 'IGMP Proxy' and 'IGMP Snooping'. Each row has two radio buttons: 'Enable' and 'Disable'. For 'IGMP Proxy', the 'Disable' button is selected. For 'IGMP Snooping', the 'Disable' button is also selected. At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

Parameters	
IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IGMP Snooping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply Cancel

**IGMP Proxy:** IGMP proxy enables the system to issue IGMP host messages on behalf of the hosts that the system has discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.

**IGMP Snooping:** Allows a layer 2 switch to manage the transmission of any incoming IGMP multicast packet groups between the host and the router. Default is set to Disable.

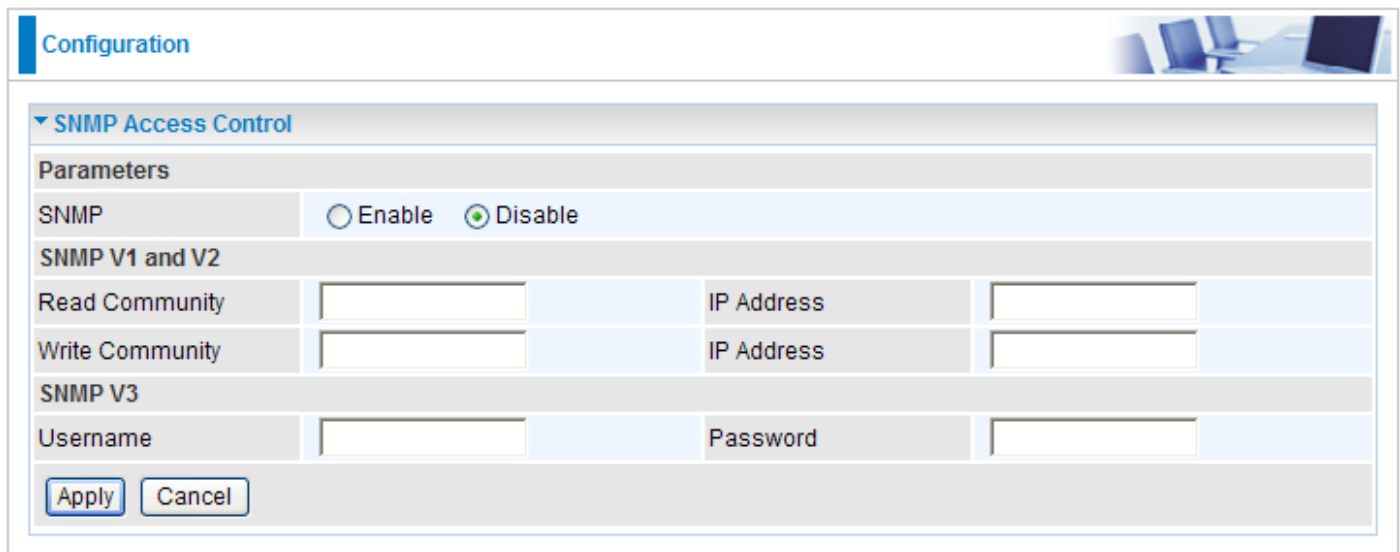
Click Apply to confirm the changes.

### Example:

*When IGMP snooping is enabled, the feature will analyze all incoming IGMP packets between the hosts that are connected to the switch and the multicast routers in the network. When the layer 2 switch receives an IGMP report from a host requesting for a given multicast group, the switch will add the host's port number to the multicast list for that multicast group to be forwarded to. And, when the layer 2 switch has detected that an IGMP has left, it will remove the host's port from the table entry.*

## SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function – Simple Network Management Protocol.



The image shows a web-based configuration interface for SNMP Access Control. At the top, there is a 'Configuration' tab. Below it, the 'SNMP Access Control' section is expanded. Under the 'Parameters' heading, there is a radio button group for 'SNMP' with 'Disable' selected. Below this, the 'SNMP V1 and V2' section contains two rows: 'Read Community' and 'Write Community', each with a text input field and an 'IP Address' label next to another text input field. The 'SNMP V3' section contains a 'Username' text input field and a 'Password' text input field. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Parameters			
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
SNMP V1 and V2			
Read Community	<input type="text"/>	IP Address	<input type="text"/>
Write Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

### Parameters

**SNMP:** Select Enable / Disable to activate / inactivate this function.

### SNMP V1 and V2

**Read Community:** Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

**Write Community:** Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

### SNMP V3

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

Click Apply to confirm the settings.



## TR-069 Client

Please contact your ISP for the information of TR069.

Configuration

TR-069 client

Parameters

Inform

☐ Enable ☒ Disable

ACS URL

ACS Username

ACS Password

Apply

Cancel

**Inform:** You may enable or disable the periodic inform feature.


**ACS URL:** Enter the ACS URL address.

**ACS Username:** Enter the ACS server login name.

**ACS Password:** Enter the ACS server login password.

Click Apply to confirm the settings.

## Remote Access

**Configuration**

**Remote Access**

**Parameters**

Remote Access Control	<input type="checkbox"/> Enable	Duration	<input type="text"/>	min(s)	(0: Always On)
-----------------------	---------------------------------	----------	----------------------	--------	----------------

**Allowed Access IP Address Range**

Valid	<input checked="" type="checkbox"/>	IP Address Range	<input type="text"/>	~	<input type="text"/>
-------	-------------------------------------	------------------	----------------------	---	----------------------

### Remote Access Control:

**Enable:** Select Enable to allow management access from remote side (mostly from internet).

**Duration:** Set how many minutes to allow management access from remote side. Zero(0) means always on.

Click Apply to confirm the settings.

### Allowed Access IP Address Range:

**Valid:** Select Valid to allow remote management from these IP ranges.

**IP Address Range:** Specify the remote IP address which will be allowed access device. Click Add to insert management IP address(es) to the list.

Click Add to confirm the settings.



# Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "Save Config" and click "Apply" to write your new configuration to FLASH.

Configuration

▼ Save Config to FLASH

Write settings to FLASH

Apply

# Restart

Click “Restart” with option Current Settings to reboot your router (and restore your last saved configuration).

Configuration

▼ Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings

☒ Current Settings

Restart

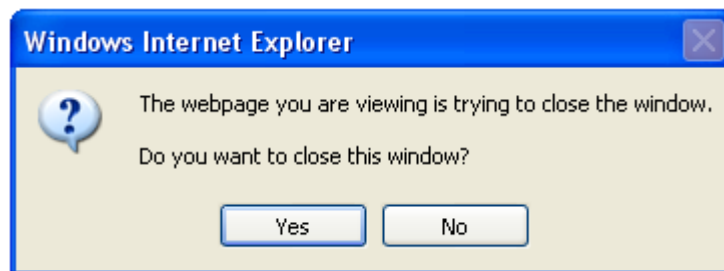
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings

# Logout

To exit the router web interface, click “Logout”. Please save your configuration setting before logging out of the system. A Warning screen will appear as below.



Click OK and a message displays. Click Yes to close the window.



Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the **Advanced** section of this manual for more information.

# Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

## Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the reset button for more than 6 seconds.

## Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.

# Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

## Contact Billion

**Worldwide:**

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP, Windows Vista and Windows 7 are registered Trademarks of Microsoft Corporation.